



CODE OF BUSINESS CONDUCT

Honeywell



Honeywell

Bank of America

LETTER FROM OUR CEO



Dear Futureshaper

At Honeywell, our Foundational Principles – Integrity and Ethics, Workplace Respect, and Inclusion and Diversity – are the driving force behind everything we do. Our Code of Business Conduct is our company-wide commitment to uphold Honeywell's principles and behaviors and achieve success with the upmost integrity. As you navigate through our company, the Code of Business Conduct is your guide to maintain our integrity and ethics.

Our dynamic portfolio and Accelerator operating system set Honeywell apart, but it is our team's commitment to the company and the company's commitment to growing and developing them that really enables our success. To build on that success, we must continue conducting ourselves with the highest levels of integrity at every level to act in the best interest of our company and each other. Acting with integrity maintains the credibility of our brand, sustains our reputation, and allows Honeywell to keep growing and innovating. This is your top priority as a Honeywell Futureshaper.

Review Honeywell's Code of Business Conduct to further understand our guidelines and how they impact your role. If you have any questions regarding the Code, you can always reach out to the resources listed to seek advice. You can always feel comfortable coming forward with any concerns. Honeywell does not tolerate retaliation against anyone asking questions or raising concerns in good faith. It is our expectation that if you observe any of your colleagues not complying with the Code, you should report your concerns immediately through one of the reporting channels listed.

Thank you for your commitment to upholding integrity and ethics at Honeywell.

A handwritten signature in black ink, appearing to read 'Vimal Kapur', with a horizontal line underneath.

Vimal Kapur

TABLE OF CONTENTS

HONEYWELL'S FOUNDATIONAL PRINCIPLES 6

ACT with Honeywell's six behaviors7

INTRODUCTION TO OUR CODE 9

What Honeywell Expects from Each of Us.....9

Who Must Follow Our Code 11

Our Shared Obligations..... 11

Additional Obligations for Managers and Supervisors 11

Complying with the Law 12

Asking for Advice 13

Reporting Channels 13

How Are Reports Handled 14

Honeywell Will Not Tolerate Retaliation..... 15

ONE HONEYWELL HOW WE TREAT EACH OTHER.....16

Respecting Each Other and Promoting a
Positive Workplace 17

Embracing Inclusion and Diversity in the Workplace 17

Protecting Personal Data 18

Substance Abuse..... 19

A Violence-Free Workplace 19

Providing a Healthy and Safe Workplace 20

ONE HONEYWELL HOW WE ACT IN THE BEST INTEREST OF OUR COMPANY21

Avoiding Conflicts of Interest 22

Gifts and Business Entertainment 22

Financial Interests 24

Secondary Employment 24

Business with Friends and Family Members 25

Improper Reporting Relationships..... 25

Improper Personal Benefits 25

Corporate Opportunities 26

Safeguarding Company Property and Information 26

Honeywell's Physical Property 26

Honeywell's Confidential Information..... 27

Honeywell's Intellectual Property	28
Respecting the Intellectual Property Rights of Others	28
Using Information Technology Resources.....	29
Responsible Use of AI.....	30
Social Media and Networking Sites.....	31
Insider Trading	32
Examples of Material Inside Information	32

ONE HONEYWELL HOW WE TREAT OUR CUSTOMERS.....33

Providing Quality Products and Services	34
Seeking Business Openly and Honestly	34
No Commercial Bribery and No Improper Payments to Government Officials	34
Compliance with International Competition Laws.....	36
Following Accurate Billing Procedures.....	37
Respecting Customer Confidential Information	37
Interacting with Government Customers	37

ONE HONEYWELL HOW WE TREAT OUR SUPPLIERS.....39

Seeking Long-Term Supplier Relationships	40
Protecting Supplier Assets	40

ONE HONEYWELL HOW WE TREAT OUR SHAREOWNERS.....41

Honest and Accurate Books and Records	42
Financial Disclosures and Fraud	43
Anti-Money Laundering	43
Audits and Investigations.....	43
Records Management	44
Inquiries from the Media and Analysts and Outside Speaking Events	44

ONE HONEYWELL HOW WE TREAT OUR COMMUNITIES AND THE WORLD 45

Protecting the Environment.....	46
Respecting Human Rights	47
Making Political and Charitable Contributions.....	48
International Trade Controls	49
Export Control Laws.....	49
Import Control Laws.....	50
Sanctions Laws.....	50
Anti-Boycott.....	50
Waivers of Our Code.....	51

HONEYWELL'S FOUNDATIONAL PRINCIPLES

Honeywell expects all employees to comply fully with the Code of Business Conduct and to abide by our three Foundational Principles: Integrity and Ethics, Workplace Respect, and Inclusion and Diversity. Our commitment to these Foundational Principles is a fundamental expectation of working at Honeywell.



INTEGRITY AND ETHICS

We do business the right way or walk away.



WORKPLACE RESPECT

We treat each other fairly and with respect.



INCLUSION AND DIVERSITY

We value diversity of thought and experiences.

While we don't expect employees to exhibit perfection at all times in all six behaviours, no one can ever fail to demonstrate Workplace Respect or Integrity and Ethics or fail to support Inclusion and Diversity. Our unfailing commitment to our Foundational Principles is a competitive advantage for the Company, and we should all take pride in our strong commitment to achieving business results the right way.



ACT WITH HONEYWELL'S SIX BEHAVIORS

In combination with achieving results, Honeywell's new behaviours will further clarify what is needed to succeed in the marketplace today and what is important in our culture.



DRIVE ACCOUNTABILITY CULTURE

Have fearless **accountability** for getting **results**. Take ownership and solve problems proactively. **Care** deeply about Honeywell and customer outcomes as individuals and as teams. Do what you say you will do. **Prioritize** and execute with discipline to drive a performance culture. **Demonstrate a bias for action and speed**.



BE COURAGEOUS

Take **bold** action on what you believe is right. Take on seemingly impossible goals and **work out of your comfort zone**. Iterate, test, try, **take measured risks**. Own results even when outcome is not as planned. Share and confront problems **openly and directly**. **Be transparent** and comfortable with being unpopular when required.



BUILD EXCEPTIONAL TALENT

Recruit, retain, and develop high quality talent. Create a positive, **inclusive** environment where people are **empowered** to do their best work. **Seek, give, and accept feedback** with the intent of making everyone better. Build robust **succession plans**. Set high standards for yourself and others. Lead by example.

ACT WITH HONEYWELL'S SIX BEHAVIORS



WIN TOGETHER

Think **ONE Honeywell** by collaborating across businesses, geographies and functions as we are stronger together. **Be a champion for our people, products, services, and solutions** and beat the competition. Be authentic, confident, and humble. **Listen** to others and be **self-aware**. Believe we can change the world **together** and create a better future for our communities. **#Futureshaper**



INNOVATE AND CREATE VALUE FOR CUSTOMERS

See the world through the **customer's** eyes, internally and externally. Know what **customers need** and what creates **value**. Have a **growth** mindset and a relentless passion for **solving tough problems**. Deliver **profitable growth** and an **exceptional customer experience** through innovative solutions. **Innovate** with agility and purpose.



EMBRACE TRANSFORMATION

Learn from and contribute to our **collective knowledge**. **Embrace digitalization** to transform the way we work. Radically simplify the complex. Use **standard processes and systems to drive operational excellence**. Drive decisions based on **facts and data**. Be **curious** and **explore** new ways of doing things to help **share the best ideas**.

INTRODUCTION TO OUR CODE

WHAT HONEYWELL EXPECTS FROM EACH OF US

Our Company's growth starts with each of us – we are key to our Company's character and central to its leadership and success.



The Honeywell Code of Business Conduct (our “Code”) is designed to provide guidance to each of us regarding Honeywell’s standards of integrity and compliance in all our business dealings. Our Code is an integral element of our Foundational Principles and the Honeywell Behaviors. It describes the basic rules of conduct that we, as One Honeywell, are expected to follow. In addition, it provides helpful resources in the event we have a question or concern about proper conduct.

Our Code defines what Honeywell expects from each of us and how we treat:



WHO MUST FOLLOW OUR CODE

Our Code applies to all employees, officers, and directors of Honeywell. Where appropriate, business partners working on our Company's behalf should also familiarize themselves with and follow our Code. If your job responsibilities require you to interact with representatives working on behalf of Honeywell, be sure to inform them of their responsibility to act in accordance with this Code and provide them with a copy. Their behavior must be consistent with our Code, other Honeywell policies, and applicable laws and regulations.

OUR SHARED OBLIGATIONS

We all have a personal obligation to know and follow the Code, as well as other Company policies, procedures, and guidelines that apply to our job responsibilities at Honeywell. Many of these are cited in the appropriate section of the Code. Others can be found in the [Honeywell Policy Manual](#). We must never ignore or seek to circumvent the Code for any reason. If you need help understanding our Code or a specific policy, procedure, or guideline, or how they apply to your scope of responsibilities, seek guidance from any resource listed in "Reporting Channels."

ADDITIONAL OBLIGATIONS FOR MANAGERS AND SUPERVISORS

Honeywell managers and supervisors have a special duty to foster a culture of compliance with our Foundational Principles. This means that managers and supervisors should serve as role models for Integrity and Compliance, Workplace Respect, and Inclusion and Diversity in all their interactions. It also means that managers and supervisors should ensure that colleagues who report to them feel comfortable raising questions and concerns without fear of retaliation, that any concerns or questions will be addressed in a professional and timely manner, and that we will not compromise our standards of integrity and compliance to obtain business results.

Managers and supervisors should also consider the character and behavior of colleagues whom they are considering for promotion. Promotions are a privilege only extended to those who exemplify Honeywell's Behaviors and values in a manner consistent with this Code.



COMPLYING WITH THE LAW

Although our Code addresses some of the common challenges that multinational companies like Honeywell face, it cannot address every situation that may arise in our workplace. When in doubt as to whether an activity is proper, you should review the resources referred to in “Asking for Advice”.

Laws and regulations are complex and subject to change, and they often vary from country to country. Company policies may also be subject to change and may vary greatly depending on the country in which we are operating. For these reasons, we must take care to familiarize

ourselves with the policies, procedures, and laws that apply to our particular job functions and to the locations in which we operate. If a local law conflicts with our Code, comply with local law. If a local custom or practice conflicts with our Code, comply with the Code.

Your business or region may have policies and practices that require more from you than required by this Code. The same may be true of local law. In all such instances, you must follow the stricter policy, practice, or law. If you have any doubts about the lawfulness or appropriateness of a proposed action, seek advice by following the steps set out in “Asking for Advice.”

This Code is intended to be consistent with and refer to certain key Corporate policies, which are included in the Honeywell Policy Manual. The Honeywell Policy Manual may provide greater detail than is provided by this Code. In some instances, the Policy Manual may provide additional policies not covered by this Code. [The Honeywell Policy Manual](#) is located on the Honeywell Digital Workplace.

It is important to note that our employment rights are governed by the laws of the countries in which we do business, as well as the rules in place in the locations where we work. Our Code attempts to clarify Honeywell’s rights and expectations as an employer but does not create any contractual employment rights for employees.

In the United States and other countries, employment by Honeywell is considered “at-will.” This means that you have the right to terminate your employment at any time and for any reason, and Honeywell may exercise the same right, consistent with applicable laws. If local laws differ from the provisions of this Code, follow the laws of the country in which you work.

ASKING FOR ADVICE

While working on behalf of Honeywell, you may face difficult situations. Many times, your common sense, good judgment, our Code, and Company policies and procedures will be enough to guide you. However, there may be times when you need additional help to make the right choice. In these instances, ask yourself:

- *Is it legal?*
- *Is this decision or action consistent with Honeywell's foundational principles, policies and the Code?*
- *Would I be willing to be held accountable for this decision or action?*
- *Would this decision or action reflect positively if reported to others within Honeywell or in the media?*

If the answer is “**no**” to any of these questions, then “don’t do it” and report the concern if you see someone else doing it.

If you are not sure, stop and consider the impact of your decisions and actions and seek guidance.

While Honeywell works hard to identify, incentivize and reward those who do the right thing, it also takes swift and decisive action—including notifying government authorities and imposing serious employment consequences, up to an including termination—against those who reject our foundational principles, violate the Code, or engage in other unacceptable conduct.

You may seek guidance by contacting any of the resources listed in “**Reporting Channels.**”

REPORTING CHANNELS

If you become aware of a situation that may involve a violation of this Code, Company policy, or any applicable law or regulation, you have a responsibility to report it.

You have several resources available to you to report these concerns.

You can either:



TALK TO:

- Your manager or supervisor
- Any Human Resources representative
- Any [Ethics Ambassadors](#)
- A member of the Law Department or Global Security
- A member of the [Integrity and Compliance Department](#)



DIAL:

800-237-5982 from the United States, and if outside the United States, refer to the [Access Integrity Helpline Portal](#) for a listing of additional country-specific helpline numbers.



ONLINE:

By submitting an online report available at the [Access Integrity Helpline Portal](#).

Email to:

AccessIntegrityHelpline@Honeywell.com



WRITE TO:

Honeywell International Inc.

Attention: ACCESS Helpline

855 S. Mint Street, Charlotte, North Carolina 28202.

The ACCESS Integrity Helpline is a 24-hour service. It is answered by an independent third-party provider that accommodates all of the languages that Honeywell employees speak.

Suspected violations may be reported by identifying yourself or by remaining anonymous. In Europe, specific processes have been implemented to comply with rules that limit anonymous reporting.

HOW ARE REPORTS HANDLED

Honeywell will treat all reports confidentially to the extent possible, consistent with the law, Company policy, and the Company's need to conduct a thorough investigation.



All reports will be investigated promptly and thoroughly, consistent with applicable law and, upon the advice and approval of the Law Department, may be reported to the appropriate authorities. Employees have a duty to cooperate with Company investigations concerning potential violations of the Code or applicable Company policies. Failure to cooperate fully in a Company investigation or to be fully truthful when providing evidence or testimony in such an investigation may be grounds for disciplinary action, up to and including termination (subject to applicable local laws). It should be emphasized that appropriate corrective or disciplinary action for Code violations will be taken whenever necessary.

HONEYWELL WILL NOT TOLERATE RETALIATION

It is important that you feel comfortable raising your questions and concerns. Honeywell will not tolerate any form of retaliation against you for making a good faith report of actual or potential misconduct. Making a report in “good faith” means your report is honest, sincere, and complete to the best of your knowledge.

If you feel an act of retaliation has occurred, you should report your concerns via one of the methods outlined in “[Reporting Channels](#).”



ONE HONEYWELL HOW WE TREAT EACH OTHER

Promoting a positive work environment based on mutual respect and a commitment to inclusivity and safety is the key to maintaining the best possible talent and to providing growth opportunities for our stakeholders.





Honeywell is committed to maintaining an inclusive, safe, and respectful working environment for all employees. Honeywell has zero tolerance for harassment or unlawful discrimination in our workplace. Such conduct is strictly prohibited. This pledge applies to all phases of the employment relationship, including hiring, promotion, demotion, transfer, discipline, layoff or termination, compensation, use of facilities, and selection for training or related programs.

RESPECTING EACH OTHER AND PROMOTING A POSITIVE WORKPLACE

At Honeywell, we are committed to treating people with respect. Employees should be able to work and learn in a safe and stimulating atmosphere where they feel valued and accepted. Together, we aim to provide an inclusive work environment that fosters respect for all coworkers, clients, and business partners and is free from harassment, or personal behavior not conducive to a productive work climate.

Honeywell will not tolerate intimidating, hostile, abusive, or offensive behaviors in our workplace. If you know or suspect that unlawful or inappropriate harassment has occurred, you should report the situation immediately via one of the reporting channels described in “Reporting Channels.”

For more information, see our [Workplace Harassment Policy](#).

EMBRACING INCLUSION AND DIVERSITY IN THE WORKPLACE

We are also committed to fostering a workplace that champions inclusion and diversity. Honeywell respects and values the diversity reflected in our various backgrounds, experiences, and ideas. Our people are our ultimate differentiator, and having employees with diverse backgrounds, perspectives, experiences, and cultures brings a diversity of ideas that supports a high-performing environment.

Our workplace is one that reflects the diversity of the communities in which we operate. We are committed to maintaining an inclusive, safe, and respectful working environment for all employees, regardless of gender, race, color, ethnic background, age, religious belief, national origin, affectional or sexual orientation, gender identity, disability, marital status, veteran status, citizenship or impending citizenship, or any other characteristic protected by law. Honeywell has zero tolerance for unlawful discrimination or conduct that otherwise singles out an employee or group of employees based on the protected categories listed above.

For more information, see our [Equal Employment Opportunity Employees and Applicants with Disabilities](#) policies.

PROTECTING PERSONAL DATA

Honeywell promotes a work environment and operates our businesses in a manner that fosters confidence and trust. To accomplish this goal, we must properly manage the personal data provided to us by our colleagues, customers, suppliers, and others. “Personal data” is any information relating directly or indirectly to an identified or identifiable natural person. Examples of personal data include: name, home address, personal email address and phone number, business contact details, HR records, employee identification number, geo-location data, log-in credentials, and online identifiers such as an IP address.

We should only collect, access, use, or disclose personal data for appropriate business purposes. In addition, we should use the minimum amount of personal data needed to accomplish a task and avoid processing personal data if the objective of the processing can be achieved without processing personal data. We must not share personal data with anyone, either inside or outside our Company, who does not have a business need to know it. Further, we must delete personal data when it is no longer needed and in accordance with the [Records Management Policy](#), and we must take steps to properly secure personal data at all times.

Company policies, practices, and training programs are designed to ensure that only authorized personnel access personal data. If you

believe that personal data has been subjected to unauthorized disclosure, use, access, destruction, or acquisition, you must contact the Law Department’s [Data Privacy Function](#) immediately. Failure to do so could subject our Company to fines and/or regulatory action.

When processing personal data, Honeywell complies with applicable law as well as Company policies.

For more information, see our

[Data Privacy Policy](#)

[Records Management Policy](#)

[Acceptable Use of Information Policy](#)

[Information Classification & Handling Policy](#)



WHAT IF...?

I need to work with a spreadsheet that has Honeywell employees’ government identification numbers. Can I send it to my personal e-mail?

No. Government identification numbers and other national identifiers constitute “sensitive identification data,” which is highly confidential, must always be encrypted, and may only be used when absolutely necessary, such as for tax purposes. Sensitive data must not be removed from Honeywell systems without the prior written approval of the Law Department.

I received a request to share personal data for insurance purposes. Should I comply?

You should verify that the requestor has an appropriate data processing agreement in place with Honeywell. In addition, you should forward the request to [HR Help](#), as only [HR Help](#) is authorized to share employee personal data externally.

SUBSTANCE ABUSE

Substance abuse limits our ability to do our work safely, which puts us all in jeopardy. For this reason, we may never work on behalf of Honeywell while under the influence of alcohol, illegal drugs, misused prescription drugs, or over-the-counter medications. This applies whenever you are performing services for, or on behalf of, Honeywell, even if the use occurs after hours or off Company premises. In addition, we may never use, possess, transfer, or sell illegal drugs, or alcohol, or misuse prescription drugs or over-the-counter medications, during working hours or while on Company premises. Our Company makes an exception to this rule when alcohol is transferred in a sealed container for authorized gift purposes or is used in moderation at an authorized Company event.

For more information, see our

[Alcohol and Drugs in the Workplace Policy](#)

A VIOLENCE-FREE WORKPLACE

We work to prevent any acts or threats of violence in our workplace as part of our commitment to health and safety. Individuals who engage in violence or threats of violence may be subject to disciplinary action, up to and including termination of employment, as well as possible criminal prosecution. You should report all threats and acts of violence to your supervisor, local Human Resources representative, or [Honeywell Global Security](#) immediately. If you feel that someone is in immediate danger, you should also contact the local authorities.

For more information, see our

[Violence Prevention Policy](#)



PROVIDING A HEALTHY AND SAFE WORKPLACE

By integrating health, safety, and environmental considerations into all aspects of our business, we protect our people and the environment, achieve sustainable growth and accelerated productivity, drive compliance with all applicable regulations, and develop the technologies that expand the sustainable capacity of our world. Our Health, Safety, and Environment, Product Stewardship, and Sustainability (HSEPS) Management System reflects our values and helps us meet our business objectives. Adherence to our HSEPS management system helps ensure that our employees, communities, and environment remain safe. Knowingly failing to comply with HSEPS requirements, including the requirement to report information regarding HSEPS incidents, is a violation of our Code. If we believe that conditions are in any way unsafe, we must stop work immediately. Refer to the section on “Protecting the Environment” for more information.

We must make sure that our facilities are secure at all times. This means we allow only authorized individuals access to our worksites. If you believe that someone is attempting to improperly access a Honeywell facility, contact [Honeywell Global Security](#).

WHAT IF...?

During a service visit, I was asked by the customer to hurry and skip a job hazard analysis, which is a crucial step. Although it goes against Honeywell guidelines, I decided to proceed without delay. Is skipping a step to please the customer appropriate?

No, skipping a required step is not acceptable. Our HSEPS Management System establishes programs such as conducting job hazard assessments to identify and manage potential risks. You should complete the job hazard assessment prior to completing the work. If the customer insists, stop work and escalate to your supervisor to find a solution with the customer.

I am the project manager for the startup of production for a new product. The project is behind schedule. During a weekly project meeting, a vendor partner mentioned that the purchase and installation of some machinery needed for the project could be expedited because the equipment is compliant with laws and no safety review is needed. To make up time, should I authorize the purchase of the new equipment without the required HSE review?

No, bypassing the review could result in violation of safety regulations and a potential safety risk to others. Always engage an HSE representative to conduct a review of proposed equipment to assure it meets all applicable legal requirements.



ONE HONEYWELL HOW WE ACT IN THE BEST INTEREST OF OUR COMPANY

We should conduct Honeywell business free from outside influences or personal biases and make business decisions based on the best interests of Honeywell.



AVOIDING CONFLICTS OF INTEREST

As part of our duty to uphold our Company's reputation, we must avoid improper conflicts of interest. A "conflict of interest" occurs when our personal interests interfere with, or appear to interfere with, our ability to perform our jobs without bias. We may not engage in any interest, investment, or association in which a conflict of interest might arise. If you have a potential or actual conflict of interest, you must disclose it immediately by speaking with your supervisor or by submitting it through the [Conflict of Interests Submission Portal](#). Conflicts of interest are often easily avoided if disclosed in advance.

The following sections describe situations that may create conflicts of interest. It is important to remember that conflicts may also be created when a member of your household or immediate family is the individual involved.

GIFTS AND BUSINESS ENTERTAINMENT

Developing strong working relationships with our customers, suppliers, and other business partners is important to our growth. Business gifts and entertainment are sometimes used to strengthen these bonds. However, we must exercise particular caution when offering or accepting business courtesies. Exchanging gifts and entertainment can result in conflicts of interests. If not handled properly, they also may lead to the appearance

of improper payments, kickbacks, or corruption. You may not accept or provide any gift, favor, or entertainment if it is made for an improper purpose or if you know it would violate our policies, the law, or the gift policy of the recipient's company.

Generally, we can offer or accept a gift, favor, or entertainment, as long as it:

- Does not make the recipient feel obligated or give the appearance of an obligation
- Does not exceed generally accepted local business practices
- Is of nominal value
- Cannot be construed as a bribe or payoff
- Does not violate applicable law, Company policies, or the policies of the recipient's company
- Is not solicited

These rules do not apply to unsolicited promotional materials of a general advertising nature, such as imprinted pencils, memo pads, and calendars, so long as what is given does not create or appear to create any obligation. Additionally, in keeping with national custom, ceremonial presentations may be permitted as long as what is accepted is not in violation of any law, cannot be viewed as a bribe, and would not embarrass you or Honeywell if disclosed.

Gifts should not be accepted from suppliers or potential suppliers (or other business partners or potential business partners) during or in connection with contract negotiations with the supplier. In addition, we should avoid soliciting gifts from suppliers or other business partners for Honeywell functions or employee awards.

If you are unsure whether you should offer or accept a business gift or entertainment, you should seek guidance. Customer entertainment and gifts must be discussed in advance with your supervisor.

Stricter laws govern gifts offered or made to government officials. These laws apply not only to government officials, but also to employees of state-owned or state-controlled companies. You must comply strictly with these laws and regulations. Never offer or accept a business courtesy if doing so violates a law or regulation, will cause embarrassment for Honeywell, or will reflect negatively on the Company's reputation. For more information, see the "No Commercial Bribery and No Improper Payments to Government Officials" section of our Code and our policies on [Business Courtesies for U.S. Government Officials](#), [Government Relations](#), and [Anticorruption](#). If you have any questions or concerns, please consult the Law Department.

WHAT IF...?

A vendor invited me to lunch, and I accepted. Is it acceptable?

Occasional meals and nominal gifts are ordinarily acceptable if they don't raise a question about your objectivity. You should request compliance approval using the employee Travel and Expense application prior to receiving or giving business courtesies.

I am planning a VIP event for customers, both private and government, where meals and gifts will be provided to the attendees. Local laws restrict the value of gifts and hospitality to certain government officials. I think it would be disrespectful to exclude certain customers, so I want to proceed with giving all attendees the same gifts. What should I do?

You should contact the Integrity and Compliance Department for guidance and approval before proceeding with the event, which should follow Honeywell policy and local law restrictions.



FINANCIAL INTERESTS

As Honeywell employees, we generally should avoid doing business with any company in which we have a personal financial interest. There may be situations where our personal financial interest in a company with which Honeywell does business is permissible. However, such situations should be reviewed by the Law Department or the [Integrity and Compliance Department](#) to determine the best course of action.

In addition, you may not purchase or maintain a significant financial interest in a customer, competitor, or business partner that does business with, or potentially does business with Honeywell, unless you receive approval from the Law Department. Always ensure you are able to make business decisions with Honeywell's best interests in mind.

SECONDARY EMPLOYMENT

From time to time, you may wish to engage in work outside our Company. In doing so, you must ensure that any outside employment does not create a conflict of interest. Nevertheless, employees are expected to treat their work for Honeywell as their primary employment. We must never use Honeywell tangible and intangible property, including documents, Information Technology assets, facilities, and intellectual property to conduct non-Honeywell business. All secondary employment should be disclosed by communicating with your supervisor or by submitting it through the [Conflict of Interests Submission Portal](#).

For more information, see our [Secondary Employment and Outside Organization Service Policy](#).

WHAT IF...?

I have been invited to join the board of a local non-profit organization that recycles and refurbishes used electronics for disadvantaged youth. There is no overlap with Honeywell's business, and my board duties occur outside Honeywell hours. Can I join?

Yes. Although there is no direct conflict, you must disclose this to your manager or HR, or through the Conflicts of Interests Submission Portal and get approval before joining. You should ensure board activities do not interfere with Honeywell duties. See the [Secondary Employment and Outside Organization Service Policy](#).

WHAT IF...?

I coach football at a community college. I want my team to make the finals, but I am also under a tight work deadline. Can I ask my direct reports to help me with the upcoming game's logistics?

No. Using Honeywell resources for an outside coaching job is inappropriate and creates a conflict of interest. You should inform your supervisor about your coaching activities and ensure they do not interfere with your Honeywell duties.

BUSINESS WITH FRIENDS AND FAMILY MEMBERS

Business relationships with family members and friends can result in a conflict of interest, or the appearance of a conflict. For this reason, you should never be involved with or attempt to influence the bidding, negotiating, or contracting process between yourself, a family member, or a close friend and Honeywell. This rule applies even in indirect situations where you, your family member, or a close friend owns or works on behalf of another company with which Honeywell does, or, is considering doing, business.

IMPROPER REPORTING RELATIONSHIPS

We need to avoid improper reporting relationships. They can lead to potential legal exposure for the Company and perceptions of favoritism and preferential treatment among the colleagues of those involved, invariably leading to an unhealthy workplace environment. Accordingly, we may not directly or indirectly supervise, influence the compensation or career progression of, or work under the supervision of, a family member or someone with whom we have a close personal relationship, whether that relationship is sexual or otherwise.

IMPROPER PERSONAL BENEFITS

A conflict of interest may also arise when a director, officer, or employee, or a member of his or her immediate family, receives improper personal benefits because of his or her position at Honeywell. Such benefits may include gifts or loans from an entity or person with whom our Company does business. We must avoid accepting any such improper benefit.

In addition, a conflict of interest arises if a Honeywell employee assists a competitor to Honeywell's detriment. For example, providing confidential information to a spouse or partner who works for a competitor would constitute a conflict of interest and violate our Code.

WHAT IF...?

I want to order parts from my cousin's company for use in a Honeywell product. Can I do this?

You should disclose your relationship to your supervisor and recuse yourself from any decision. If your cousin's company meets Honeywell's standards, it can compete fairly for the order

WHAT IF...?

I need to hire someone quickly and have asked my job-seeking cousin to apply. Is it ok?

This could appear as a conflict of interest. You should disclose your relationship and not be involved the hiring. Standard staffing and management processes must be followed.

WHAT IF...?

I started my own business and need to understand pricing details of potential suppliers to my business. Would it be wrong to pull the pricing data of some of these potential suppliers from the Honeywell system?

Yes. It creates a conflict of interest. You cannot use Honeywell information or perform work for a personal business on Honeywell premises or during your working hours. In addition, you should not use Honeywell's suppliers' confidential information for a non-authorized purpose.

CORPORATE OPPORTUNITIES

In order to make objective business decisions on behalf of Honeywell, we must never compete with our Company. This means we may not take for ourselves any business or investment opportunities that we discover through our position at Honeywell or through Company property or information. In addition, we must never help anyone else take such business or investment opportunities for personal gain. This includes our family members and friends.



SAFEGUARDING COMPANY PROPERTY AND INFORMATION

HONEYWELL'S PHYSICAL PROPERTY

Theft, damage, carelessness, and waste have a direct impact on our Company's success. We must therefore commit to protecting our Company's physical assets from theft, damage, loss, or misuse. This includes our facilities, vehicles, business equipment, merchandise, and supplies. If you suspect any form of fraud or theft, you should report it to your manager or supervisor immediately.

Authorized occasional personal use of certain Company equipment, such as telephones or internet, is sometimes appropriate. However, we must ensure our personal use is limited, does not interfere with our ability to do our work for Honeywell, and does not violate Company policy or law. Never use Honeywell property for personal gain or that of another person or organization. You must also return any Company property you possess at the end of your employment.



HONEYWELL'S CONFIDENTIAL INFORMATION

We are each entrusted with our Company's confidential information. We must protect this sensitive information at all times. This generally includes any nonpublic information that might be of use to competitors or others, or which may be harmful to the Company if disclosed. Examples include business or marketing plans, supplier information, product design, manufacturing processes, existing and future merchandising information, and employee information.

We must never allow unauthorized personnel to access Honeywell's confidential information. We must take care not to lose, misplace, or leave confidential information (or technologies containing such information, including computers, laptops, cell phones, mobile devices, and software) unattended. Moreover, if we lose Company equipment or an item containing confidential Honeywell information (for example, a Honeywell laptop, phone, or the like), we should report the loss immediately to

[Honeywell Global Security](#).

In addition, we may not discuss Honeywell's confidential information where it might be overheard or seen by those who do not have a need to know it. This includes public places such as airport terminals, trains, and restaurants. It also includes open areas at Honeywell such as Company restrooms and break rooms. We may only grant access to confidential information to coworkers who have a legitimate business need to know it. We must never use confidential information about the Company for personal gain or disclose it to others for their gain. We must never email Honeywell confidential information to a personal email account, and we must return any Honeywell's confidential information in our possession before our last day of employment.

For more information, see our

[Data Privacy Policy](#)

[Information Classification and Handling Policy](#)

WHAT IF...?

My laptop was stolen when someone broke into my vehicle. What should I do?

You should file a police report, notify your manager, and file a Lost/Stolen Laptop form or contact IT Service Desk to obtain assistance to file the form. Employees should not leave devices in an unattended vehicle even if locked.

I suspect my system has been compromised after clicking a link in an email that appeared to be legitimate. What should I do?

You should use the "Report Message" button on your Outlook toolbar to report the email, or if not available, send the email in question as an attachment to [CIRT](#) (Cyber Incident Response Team). You should escalate the incident by replying to the automated email response sent from the [CIRT](#) mailbox and copy Security@Honeywell.com.



HONEYWELL'S INTELLECTUAL PROPERTY

We work diligently to protect our Company's intellectual property. "Intellectual property" includes any of our Company's patents, trademarks, copyrights, or other intangible assets such as, ideas, inventions, processes, or designs created on Company time, at Company expense, using Company resources, or within the scope of our job duties. We will identify any new inventions we make and will direct them to the Law Department for patent, copyright, or trade secret protection. You should report any suspected misuse of our Company's intellectual property to the Law Department.

RESPECTING THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS

We respect the intellectual property rights of others. This means we must never knowingly infringe on the copyrights, trademarks, or patents of others. We may not download unlicensed software onto Company computers or duplicate, publish, or distribute copyrighted materials. We will not download songs, photographs, and videos without consent from the rightful owner. In addition, we will not disclose or use the confidential information of former employers.

See our [Licensing of Honeywell Intellectual Property Policy](#) for more details.

WHAT IF...?

I often work and take business calls in public areas. Can I discuss Honeywell business this way?

You can take calls in public places, but you should not discuss any proprietary or confidential information.

I want to use my device to review and work on business-related documents while using public transportation. Is this a problem?

It may be. When using company devices in public places for Company business, you must always protect your screen from onlookers. You must also lock and secure your workstation when not in use. Be sure to secure any connections to public Wi-Fi by connecting your device to your Virtual Private Network (VPN).

USING INFORMATION TECHNOLOGY RESOURCES

Honeywell provides many of us access to various electronic communications systems to use in our daily work. This includes computer and phone systems, laptops, cell phones, mobile devices, and software. We have a duty to safeguard these systems and the technologies provided to us at all times. This means we must each do our part to prevent damage, harm, loss, and unauthorized access to these resources. Be sure to follow all security measures and internal controls in place for the resources you use. Always lock and secure your workstation, laptop, or mobile device if left unattended in a public place or at a Honeywell location even if for a short period of time. Safeguard your login credentials to all Honeywell devices and accounts. Never share your credentials with any unauthorized agent. Where required to share your password to an authorized agent for technical support purposes, change your password immediately once your technical issue has been resolved.

Remember that electronic messages (such as emails, instant messages, and text messages) are permanent records of your communications. These communications can be altered and forwarded without your permission. For this reason, take particular care when drafting any electronic messages or letters on Company letterhead or when using Honeywell resources.

Exercise good judgment and integrity when using these systems and technologies. Only use approved systems, devices, storage media, and/or services to process, store, or transmit Honeywell information. Do not install unapproved software on Honeywell computers, network servers, or other Honeywell Information resources without receiving advance authorization from Honeywell IT. Do not agree to any third-party agreements such as cloud or clickthrough services agreements on behalf of Honeywell. Do not download or send inappropriate, sexually explicit, illegal, or offensive material via these resources. You also may not use these resources to conduct outside work. To the extent permitted by local law, you should not have an expectation of privacy when using Company resources, as Honeywell may monitor your personal use of Company resources. However, it is important to note that our Company will not interfere in our personal lives unless our conduct is prohibited by law, impairs our work performance, or adversely affects our work environment or Honeywell's reputation.

For more information, see our [Acceptable Use of Information Policy](#).

WHAT IF...?

I am working in a coffee shop using a Honeywell device. After finishing work, I connect to a personal Wi-Fi to download my favorite TV show. Is this appropriate?

Limited non-business use, which is not an abuse of Company time and/or resources and follows all Honeywell policies can be permitted at the manager's discretion. Employees should always act in an ethical and lawful manner and always obtain manager permission to use a Honeywell asset for non-business use. To avoid cybersecurity threats, never use open public Wi-Fi networks because these are not protected. Where such connections are the only option, VPN must be used.

I need to share sensitive information with a supplier to complete a project, and the supplier suggested I upload the files to a third party's cloud system. What should I do?

You should use Honeywell IT approved transfer methods first. If another method is needed, work with Honeywell IT for approval. Note that export-controlled and restricted data can never be moved into any cloud service. Contact your [Export Compliance Officer](#) for guidance.

RESPONSIBLE USE OF AI

Honeywell is committed to the responsible use of AI and Generative AI, and we incorporate principles of accountability, safety, reliability, fairness, privacy, protection of intellectual property, transparency and sustainability to inform decision making across all AI uses at Honeywell. While the Company encourages innovation through the use of AI tools, you must obtain appropriate approvals for new AI or Gen AI use cases when required and only use authorized AI tools that are provided to you by Honeywell for work purposes.

For more information, please refer to the

[Honeywell Responsible AI Governance Framework](#)

[Honeywell Responsible AI Policy.](#)



WHAT IF...?

I want to use an AI tool to assist me with my work including summarizing and drafting work emails. Can I do it? And can I use my personal email address or account to access public GenAI tools for work purposes?

We encourage you to use AI to maximize innovation and gain efficiencies as long as you do so by using AI tools approved by Honeywell such as Microsoft 365 Copilot, which can help you summarize and draft emails. Other approved tools, like HON GPT, are listed in the [Generative AI Standard](#). You may **NOT** use public GenAI tools for work purposes, nor may you circumvent security controls and policies put in place to protect Honeywell data such as by using your personal email address or account for work purposes.

SOCIAL MEDIA AND NETWORKING SITES

Social media has changed the way many of us share information on a daily basis. While social media create new opportunities for communication and collaboration, such media also brings additional responsibilities that we must know and follow. “Social media” sites include a vast array of websites and online resources. These include social networking sites (such as Facebook, Twitter, Instagram, Snapchat, YouTube, and LinkedIn), blogs, photo and video sharing sites, forums, and chat rooms, among many others. If your position at Honeywell requires posting on such sites, as a representative of Honeywell, you must only do so for authorized Honeywell business purposes and only post information that complies with this Code and Company policies. In your personal “social media” interactions, act responsibly. What you post can adversely affect Honeywell’s reputation. Be careful to protect our reputation at all times. Never post confidential information about Honeywell or our colleagues, customers, suppliers, or business partners on any such sites.

For more information, see our

[Social Media Policy](#)



WHAT IF...?

I am excited about a potential new business project for Honeywell. I want to share the news on my Facebook account. Is this a problem?

Yes. Honeywell employees are not allowed to share confidential or proprietary information regarding the Company’s potential ventures on their social media networks or otherwise.

I am thrilled about a business deal that is showcased on the Honeywell website. I want to share it on my LinkedIn and Twitter accounts. What is the right way for me to share this news in my social media?

If you listed Honeywell as your employer and you include a disclosure of your relationship to Honeywell on your post, you can share a link to the Honeywell.com article. You can also share any posts that appear on official external Honeywell channels.

I am reading an article online that contained inaccurate information about Honeywell products. I quickly respond in the comment section to correct such statement. Is that appropriate to do?

You are not authorized to speak on behalf of Honeywell. Instead, you should notify your manager and the Communications team, who will determine whether and how to respond.



INSIDER TRADING

Honeywell policy establishes standards for employees and others who have material inside information and prohibits insider trading. During the course of your work with Honeywell, you may learn about material inside information regarding Honeywell or another company that is not yet public. Using this information or conveying this information to others for financial or other personal gain is a violation of our insider trading policy and may also violate securities laws. Such laws make it unlawful for any person who has “material inside information” about a company to trade the stock or other securities of that company or to disclose such information to others who may trade. Violations of such laws may result in civil and criminal penalties.

EXAMPLES OF MATERIAL INSIDE INFORMATION

“Material inside information” is information that is not generally available to the investing public and, if disclosed, would reasonably be expected to affect the price of a security or would influence your decision to buy, sell, or hold a security. Examples of material inside information may include: unannounced earnings; mergers, acquisitions, and dispositions; the outcome of major litigation; a change in control; a change in senior management; or a significant cybersecurity event. This list of examples is not exhaustive and material inside information may arise in connection with other events not listed here. You should consult the [Insider Trading Policy](#) for a more detailed discussion on material inside information.

To avoid violating our insider trading policy and securities laws, DO NOT:

- Buy or sell shares in any company, or recommend buying or selling shares in any company, including Honeywell, either directly or through family members or other persons or entities, if you have material inside information about that company.
- Convey material inside information to others outside the Company unless it is necessary for the Company’s business activities, and it is conveyed under confidentiality protections.

Certain individuals, because of their positions with the Company (including the Company’s directors, officers, and other key employees involved in certain financial and other forecasting activities), are viewed as possessing material inside information and are designated as “insiders.” These individuals are subject to additional restrictions (such as pre-clearance authorization) which are more fully described in the [Insider Trading Policy](#).

If you have material inside information about a company (including Honeywell), you may only trade in that company’s securities once the information is made publicly available to ordinary investors through appropriate media sources.

If you have questions or need guidance in this area, please consult the Law Department.

ONE HONEYWELL HOW WE TREAT OUR CUSTOMERS

Building mutually beneficial relationships with our customers is important to our success as a Company. Maintaining such relationships requires that we provide safe, quality products and uphold the law in all our interactions with both commercial and government clients.





PROVIDING QUALITY PRODUCTS AND SERVICES

We strive to provide products and services that meet or exceed our customers' requirements for quality, reliability, and value.

We are expected to comply with all quality control standards that govern our job duties. This includes applicable laws and regulations, as well as internal control procedures designed to promote the safe, quality manufacture of goods. We are also expected to follow all contract specifications and honor built-in client specifications at all times.

In addition to holding ourselves accountable for quality goods and services, we must also hold our suppliers and other business partners accountable to ensure the quality of the products and services they provide to us.

WHAT IF...?

I discovered a potential product safety problem during routine production line testing. Should I speak up about this, even if I don't know all the details?

Yes. Producing and selling potentially unsafe products could result in injury. You should report the problem immediately, even if you aren't sure if it is an issue. You should make your supervisor, quality assurance contact, or health and safety representative aware of the issue as soon as possible. If you believe your concerns are not being adequately considered, you should report the concern to the Law Department or via the Access Integrity Helpline, as discussed in "Reporting Channels."

SEEKING BUSINESS OPENLY AND HONESTLY

Our actions in the marketplace define who we are as a company. By competing on the quality of our goods and services, we uphold Honeywell's reputation. We will never seek to limit the competitive opportunities of our rivals in deceitful or fraudulent ways.

In addition, we never take advantage of anyone through unfair dealing practices. This means that we are careful not to misrepresent the quality, features, or availability of our products or services. In addition, we do not disparage or make untrue statements about our competitors' products or services. We seek to win business based on the quality of our products and our people, not through any improper means.

NO COMMERCIAL BRIBERY AND NO IMPROPER PAYMENTS TO GOVERNMENT OFFICIALS

We should not solicit, give, or receive commercial bribes or unlawful kickbacks. We should also be careful to avoid even the appearance of such improper conduct. "Commercial bribery" generally includes any situation where a Honeywell employee or someone acting on Honeywell's behalf offers or gives something of value with the intent to improperly influence a business action or decision. Unlawful "kickbacks" generally include any situation where an employee receives an improper personal benefit in exchange for taking or refraining from taking an action on behalf of Honeywell. Honeywell will not tolerate commercial bribery or unlawful kickbacks, whether it is done directly or through a third party.

In addition to avoiding commercial bribery and unlawful kickbacks, we comply with all applicable anticorruption laws regarding improper payments to government officials. "Improper payments"

include both direct and indirect payments, facilitation payments, or an offer, promise or authorization of a payment or anything of value to a government official for purposes of improperly influencing government acts or decisions in order to obtain or retain business or otherwise secure a business advantage. Note that improper payments can take the form of cash, gifts, or lavish entertainment.

“Government officials” include officials of government entities, international organizations and political parties, employees of state-owned companies, and even employees of government-owned or controlled companies and joint venture partners.

Honeywell prohibits improper payments to government officials. It is important to remember that engaging in bribery, or even appearing to engage in such activity, can expose you and our Company to criminal liability.

Never retain a third party to make an improper payment to a government official or enter into any transaction where you suspect a third party is making such payments. Doing so violates our Code and anticorruption laws. We must carefully screen all third parties using our due diligence procedures before retaining them.

Honeywell’s obligation to report potential concerns regarding the Code is especially critical in this area in light of reporting requirements Honeywell possesses under the Deferred Prosecution Agreement that it entered into with the Department of Justice in 2022 involving interactions with Petrobras. Any] concerns related

to this topic should be raised through proper channels, including directly with the Regional Integrity and Compliance resources in your region.

For more information, please see our

[Anticorruption Policy](#)

and the [“Gifts and Business Entertainment”](#) section of our Code.

WHAT IF...?

I would like to appoint Sales Rep Co as a sales representative to help Honeywell win new projects in the oil and gas industry. I find out that the owner of Sales Rep Co is also a board member of the state-owned oil and gas company, my key potential customer. I think this is great for Honeywell because the owner would have access to all levels of the customer. Is there anything I should be concerned about?

Yes, there is a potential conflict of interest related to the overlap of official duties of the owner of Sales Rep Co with the Sales Rep Co.’s duties to Honeywell. You must immediately contact the Integrity and Compliance Department. In addition, Honeywell prohibits commission-based compensation structures for sales representatives unless (i) required under local law, and (ii) approved by the Integrity and Compliance Department.

I am concerned that Honeywell will likely lose a big contract if she doesn’t pay a local official a bribe. It appears our competitors are not limited like we are at Honeywell.

What should I do?

By Honeywell policy and by law in all areas that we do business, it is inappropriate and not legal pay a bribe or take any actions that would transfer a benefit to a government official, directly or through an intermediary, including a vendor. No contract is worth violating the law or our standards of business integrity. The potential long-term damage to Honeywell’s reputation and credibility more than offsets the short-term gain of winning the contract. Often rumors that competitors play by different rules are unsubstantiated or result in those companies suffering negative consequences ultimately. We act consistent with our values and the Code and do not justify our actions based upon potential lower standards other companies may employ.

WHAT IF...?

I am waiting to enter a country when the immigration official asks me for a 'donation' for my visa to be processed. I heard that this is the norm, and visitors give a small amount to expedite the process. I pay the 'donation' to the official, and he stamps my passport. Can I get it reimbursed by Honeywell?

No, in this case, your life was not in danger, so you should not have paid and cannot claim money back from Honeywell. Facilitation payments or payments to officials to expedite routine government approvals are prohibited by Honeywell unless the employee's life is in danger. Such fees are a violation of anti-corruption laws in most countries. In such situations, Honeywell employees should contact Global Security or the Integrity and Compliance Department.

COMPLIANCE WITH INTERNATIONAL COMPETITION LAWS

Fair competition creates a healthy marketplace. It ensures our clients the best and most innovative products and services at the lowest prices. In order for Honeywell to compete lawfully and with integrity, we must comply with the competition laws in place in the countries where we do business. If competition

laws apply to your job function, you must know and follow them at all times.

Competition laws are often complex, and generally forbid discussing any topics with competitors that may restrain trade. Such topics include (but are not limited to) price fixing, bid rigging, or dividing or allocating markets, territories, or clients. You should not discuss any of these topics with a competitor, and if a competitor attempts to discuss any of these topics with you, you must stop the conversation immediately. Then, you should report the incident to your local supervisor, who will work with you in consultation with our Law Department. If you are attending a trade association meeting, or a social event, for example, exercise particular caution during discussions with competitors.

In addition, competition laws prohibit formal or informal agreements with suppliers, distributors, or clients that may restrict competition. Such agreements may include tying products, fixing resale prices, or refusing to sell to particular clients or buy from particular suppliers.

Finally, competition laws prohibit direct or indirect, formal or informal, agreements between or among companies to limit employee wages or benefits. Accordingly, we must be careful not to share compensation data with other companies with whom we compete for talent. Likewise, we generally may not agree with other companies not to solicit or hire each other's employees. If you are uncertain whether any such information sharing or "no-poaching" agreements are illegal, please consult the Law Department.

Through our work, we may obtain competitor information from our customers or other public sources. We must be particularly careful to handle this information in accordance with Company policy.

Please note that violating these laws may subject both the individuals involved and our Company to severe consequences.

WHAT IF...?

My friend works for a Honeywell competitor. He reveals to me his company's intent to raise prices on products that are in direct competition with Honeywell's. I feel this information could be important for Honeywell to use in making future business decisions. What should I do?

You should end the conversation immediately and provide a written summary to the Law Department. Engaging in discussions with competitors on nonpublic, competitively sensitive information could create the impression of an illegal, anticompetitive agreement between the companies, which could have serious consequences for all involved, including providing circumstantial evidence of a conspiracy

For more information, please see our

[Antitrust Compliance Policy](#). If you have any additional questions, seek guidance from our Legal Department before acting.

FOLLOWING ACCURATE BILLING PROCEDURES

Our reputation in the marketplace is a critical Company asset. For that reason, we reflect accurately on all invoices to customers the sale price or cost of goods or services sold and other terms of sale. We each have a responsibility to maintain accurate and complete records in order to allow Honeywell to uphold this commitment. Never falsify any record – timecard, expense report, sales numbers, test or quality records, or any other kind of record created during the course of your work for our Company – or make misleading or artificial entries on Honeywell’s books or records.

RESPECTING CUSTOMER CONFIDENTIAL INFORMATION

At times, our customers may share their confidential information with us so that we may provide them with products and services. It is our responsibility to use, store, and carefully safeguard any such information in a manner that complies with all applicable laws. We each must take the necessary steps to secure this information and ensure it is used only for approved business purposes.

INTERACTING WITH GOVERNMENT CUSTOMERS

For some of us, our work involves contracts with government entities, including government-owned or controlled companies. In these cases, we have a duty to know and follow applicable Company policies and the established laws, rules, and regulations that govern our interactions with government customers. It is important to note that these rules may be stricter and more complex than those governing our dealings with commercial clients.

We must always conduct ourselves with honesty and integrity when attempting to win government work. This means, in part, that:

- We may not take actions that would give Honeywell an unfair competitive advantage, such as obtaining or using sensitive procurement information.
- All representations we make, including pricing and bids, must be accurate and complete.
- We must never offer, solicit, promise, give, or accept any form of bribe or kickback to or from an actual or potential government customer.
- We must never solicit or accept any form of bribe or gift from a supplier in exchange for favorable treatment in the award or performance of a government contract.

- We must ensure we only use reputable consultants, sales agents, or other professional service independent contractors for legitimate legal purposes.

For more information, please see our

“No Commercial Bribery and No Improper Payments to Government Officials” section of our Code and our [Business Courtesies for U.S. Government Officials](#), [Government Relations](#), and [Anticorruption](#) policies.



All statements and records that we provide to government customers (including facility and quality reports and cost and pricing data) must be accurate. We must record our time accurately and identify and assign our time only to projects on which we work. In addition, we must take care to avoid mischarging any costs. We must follow all contract terms and may never use government property, equipment, or supplies in a manner that would be inconsistent with applicable law or contractual agreements.

We must follow all applicable rules and regulations that govern how we engage current or former government employees in discussions about potential job opportunities at Honeywell. We are each responsible for avoiding these types of conflicts of interest. Contacting or engaging in employment-related discussions with current or former government employees is subject to unique rules and procedures. These rules may also restrict the work that former government employees perform on our Company's behalf.

Please refer to our [Hiring or Engaging Former Government Employees Policy](#).

We also are expected to safeguard classified and other sensitive information we acquire in connection with the work we do for our government clients. As required by the terms of our government contracts and other applicable regulations, we make this information available only to those who have a business need to

know it and who have obtained the appropriate government clearance or other approvals. We must not share, distribute, or disclose classified or otherwise sensitive government information in a manner that would violate the terms of our government contracts.



ONE HONEYWELL HOW WE TREAT OUR SUPPLIERS

Honeywell's suppliers are our partners in our ongoing drive for customer satisfaction. The high caliber of the materials, goods, and services they provide is linked directly to the quality, reliability, value, and prompt delivery of Honeywell products to our customers.



SEEKING LONG-TERM SUPPLIER RELATIONSHIPS

Together, we strive to build long-term relationships with our suppliers. We only use legitimate, business-related criteria when choosing suppliers. Our Company will enter into representation or supplier agreements only with companies believed to have demonstrated a record of and commitment to integrity. In addition, we never take unfair advantage of our suppliers through abuse of confidential information, misrepresentation of material facts, or any other unfair dealing practice.

At Honeywell, we allow suppliers to compete fairly on the quality of their products and services. We will not be influenced by gifts or favors of any kind from our suppliers or potential suppliers. An occasional meal or entertainment in the normal course of business relations may be permissible, as long as:

- The representative of the supplier is in attendance.
- Such hospitality is not excessive or unusual in nature.
- The hospitality complies with applicable laws and is not otherwise prohibited by this Code.

In addition, when practical, hospitality should be reciprocated.

For more information, see the

[“Gifts and Business Entertainment”](#) and [“Interacting with Government Customers”](#) sections of our Code.

PROTECTING SUPPLIER ASSETS

We treat supplier confidential information with the same care as we treat Honeywell confidential information. We will not reproduce software provided to us by a supplier, nor will we incorporate it into our own internally developed software unless we are expressly permitted to do so by license.



ONE HONEYWELL HOW WE TREAT OUR SHAREOWNERS

At Honeywell, we strive every day to build value for the shareowners who have placed their trust in our Company and in each of us. To achieve this goal and create value for our shareowners, we must do business with transparency and integrity.



HONEST AND ACCURATE BOOKS AND RECORDS

Our shareowners rely on us to maintain accurate and complete books and records. These documents form the basis for all of our public disclosures and filings, which aim to give our shareowners and the public an accurate view of our Company's operations and financial standing. In addition, Honeywell uses these documents to analyze Company operations and make important business decisions.

We have a duty and a legal obligation to make sure that the information we submit in all Company records is complete, accurate, and understandable. This includes, but is not limited to, all of the information we provide in the following records:

- Accounting and financial records
- Payroll documents
- Timecards and time recording systems
- Travel and expense reports
- Measurement, product testing, and performance records
- Customer and supplier records
- Design and engineering records
- Export and import declarations and records
- Project accounting records

Honest and accurate books and records play a significant role in our Company's reputation. As such, we must never make a false or misleading representation in any Company documents.

Our Company's transactions will be executed only in accordance with management's general or specific authorizations. See our [Delegation of Authority Policy](#) and [Schedule of Executive Approvals](#) for more information.

WHAT IF...?

I am working on a government contract project. and I need my manager's approval for my weekly timesheets, but my manager is on vacation. Can I approve my timesheets on behalf of my manager?

No. Approving your own time sheets represents a segregation of duties conflict and jeopardizes management controls. Your manager should ensure appropriate delegation of his/her approval duties.

I need to process a purchase order for an amount that triggers senior executive approvals. Can I split the purchase order to get through the system more quickly?

No. All transactions must be executed according to the Schedule of Executive Approvals and must reflect the business nature. You should never split a purchase order.

I am helping to develop new technology for military aircraft. Honeywell must certify to the customer that the new technology meets required technical standards. Can I certify to the customer prior to completing the work that the technology meets the required standards?

No. Every Honeywell representation must be accurate at the time that it is made. This includes certifying compliance to specific technical standards.

Account managers are struggling to meet their quarter-end revenue targets. They have upcoming orders, but the customer is not ready for shipment yet. Can they bill the customer and hold the shipment until the customer is ready to receive it in order to recognize revenue? ?

No. Transactions where Honeywell recognizes revenue upon the sale, but the product remains in Honeywell's physical possession (i.e., "bill and hold.") can sometimes be legitimate. But in this case, the account managers want to bill the customer without shipment to inflate revenue, which is not appropriate.

FINANCIAL DISCLOSURES AND FRAUD

Those of us with finance and accounting responsibilities have a special duty to ensure that our Company's financial statements are true and fair. Since Honeywell is a U.S.-based public company, we must submit various financial reporting and other filings to U.S. regulatory authorities. It is critical that these documents are accurate and timely. Therefore, if you have related responsibilities, you must comply with the legal and regulatory requirements that govern these reports. You also must know and follow Honeywell's internal controls that govern the same. Inaccurate, incomplete, or untimely records or reporting may result in legal liability for the Company and for those involved.

Anyone found to have engaged in financial fraud will be subject to disciplinary action and could face substantial civil and criminal liability. You must report any suspected accounting or auditing irregularities immediately. Honeywell will not tolerate retaliation against you for disclosing, in good faith, questionable or improper accounting or financial matters.

ANTI-MONEY LAUNDERING

Money laundering is the process of transforming the assets (including, but not limited to, funds or proceeds) of criminal activity into assets that look legitimate and can be moved through the financial system without suspicion. It is important to note that this practice is not limited to cash transactions. Complex commercial trade transactions may hide financing for criminal activity such as terrorism, illegal narcotics trade, bribery, and fraud. Involvement in such activities undermines our integrity, damages our reputation and can expose Honeywell and individuals to severe sanctions.

Our Company forbids knowingly engaging in transactions that facilitate money laundering. We take affirmative steps to detect and prevent engaging in transactions with disreputable counterparties and/or participating in suspicious or illegal commercial transactions and payments. Honeywell is committed to compliance with anti-money laundering laws throughout the world and will conduct business only with permissible parties involved in legitimate business activities and transactions.

For more information, please review the [Anti-Money Laundering Policy](#).

AUDITS AND INVESTIGATIONS

We all share a responsibility to cooperate with external and internal audits and investigations. This means we must provide auditors and investigators the information to which they are entitled and maintain the confidentiality of the investigation. In addition, we may never attempt to interfere with or improperly influence their review. Refusal or failure to cooperate fully with an internal Honeywell or government investigation, or the failure to be fully truthful when providing evidence or testimony in such investigation, may result in disciplinary action, up to and including termination. If you have any questions about what information an auditor or investigator is requesting and entitled to obtain, consult with the Law Department or Corporate Audit. If contacted regarding a governmental investigation, you must contact the Law Department as soon as possible before proceeding. The Law Department will have primary oversight over any internal investigation or audit involving a governmental investigation or litigation matter.

RECORDS MANAGEMENT

It is our shared responsibility to retain Honeywell business records as long as needed for business purposes or longer, if required by law, tax, regulatory, or other standards. In addition, we need to know when and how to destroy these business records appropriately. Employees must follow all rules set forth in our [Records Management Policy](#). The [Records Management Policy](#) includes the Records Retention Schedule, which provides guidance regarding the length of time various records should be retained. Honeywell encourages employees to review their records on a regular basis and to purge old documents in accordance with the [Records Management Policy](#). Purging documents in compliance with our Policy helps to reduce records storage costs, but it is critical to do so in accordance with document destruction rules.

If you know that documents in your control may be relevant to a lawsuit or government investigation, do not alter, conceal, or destroy them. In some cases, the Law Department may instruct you to preserve certain documents that might otherwise be destroyed under Honeywell's [Records Management Policy](#). In such cases, you should follow the instructions provided by the Law Department.

Time sensitive and important legal and business mail and other forms of correspondence may be received by Honeywell at any of its offices globally. All Honeywell employees must take steps

to open, review, and process all correspondence in a timely manner, regardless of the method of delivery. If you become aware of any actual or potential legal proceeding or investigation involving Honeywell, you must immediately notify a member of the Law Department, and you must do so before engaging with a third party on same.

TIP

If you receive a legal notice of any type through Company mail, email, or any other means of communication, you must report it immediately to the Law Department and/or your manager for immediate escalation.

INQUIRIES FROM THE MEDIA AND ANALYSTS AND OUTSIDE SPEAKING EVENTS

We strive to provide clear and accurate information to the media, financial analysts, and the general public. This helps us maintain integrity in our relationships with our external stakeholders, which in turn strengthens our corporate reputation. Since accurate information is so crucial, only certain individuals are permitted to communicate with the media, financial analysts, and members of the investment community on Honeywell's behalf. If you receive a request for information from the media, forward it to Corporate Communications. If you receive a request from a financial analyst or member of the investment community, do not

respond on your own, but rather, forward it to Investor Relations for handling.

Any Honeywell employee who wishes to present a Honeywell product, system, operating method, research, or their own work at an industry conference or other event must get approval in advance from their direct supervisor and the Law Department. Presentations must (i) be consistent with current Company brand standards; (ii) be consistent with the Company's Investor Relations messaging; (iii) be consistent with Company strategy; and (iv) not impart confidential or proprietary information. Additional approvals are required for presentations related to cybersecurity or environmental, social and governance (ESG) matters.

For more information, please see our [External Communications Policy](#)

ONE HONEYWELL HOW WE TREAT OUR COMMUNITIES AND THE WORLD

In order to grow as a Company, we must work to have a positive impact on the communities that sustain us. We must work to respect and protect not only the communities where we live and work, but also our planet and its inhabitants.



PROTECTING THE ENVIRONMENT

We are committed to health, safety, and the environment, and to social considerations in the communities in which we operate. As part of this commitment:

- We minimize the environmental footprint of our operations through prevention of illness, injury, and pollution.
- We actively promote and develop opportunities for expanding our sustainability profile by increasing energy, fuel and water efficiency, improving security and safety, and reducing emissions of harmful pollutants.
- We are committed to compliance with all our health, safety, environmental, and legal requirements everywhere we operate.
- Our commitment to health, safety, and the environment is an integral aspect of our design of products, processes, and services, and of the lifecycle management of our products.
- Our management systems apply a global standard that provides protection of both human health and the environment during normal and emergency situations.

- We identify, control, and endeavor to reduce hazards and associated risks (to employees and contractors), emissions, waste, and inefficient use of resources such as energy and water.
- We are open with stakeholders and work within our communities to advance laws, regulation, and practices that safeguard the public.
- We abide by our Company's own strict standards in cases where local laws are less stringent.
- Our senior leadership and individual employees are engaged in aspects of health, safety and the environment and are accountable for their role in meeting our commitments.
- We measure and periodically review our progress and strive for continuous improvement.

If you have a concern about workplace health, safety, or environment, please contact your local supervisor, a member of the Health, Safety Environment, Product Stewardship and Sustainability function, or visit the [HSE website](#).



RESPECTING HUMAN RIGHTS

At Honeywell, we are committed to supporting human and workplace rights in our global operations and supply chain. We believe that workers should be treated with fairness, dignity, and respect, and we seek to ensure that every employee has a voice in our workplace. This commitment is grounded in international human rights principles that independent organizations have proposed, such as the United Nations Guiding Principles on Business and Human Rights, Ten Principles of the United Nations Global Compact, the International Labor Organization's Declaration on Fundamental Principles and Rights at Work, and all applicable laws of the jurisdictions where we operate.

Our Code and our [Human Rights Policy](#), along with other Honeywell policies, establishes practices and standards that address a broad range of human rights and workplace issues, such as Inclusion and Diversity, Workplace Respect, Freedom of Association, Safe and Healthy Workplace, Workplace Security, Work Hours and Wages, Forced Labor and Human Trafficking, and Child Labor. Honeywell respects and values the diversity reflected in our various backgrounds, experiences, and ideas. Together, we provide each other a diverse and inclusive work environment that fosters respect for all of our coworkers and business partners. Refer to the section titled "Respecting Each Other and Promoting a Positive Workplace" for more information.

Our Company does not condone or employ child labor. At Honeywell, we will not employ anyone under the age of sixteen, even if authorized by local law. If local law is stricter than Company policy, we will comply with that law. In addition, we will never use forced, indentured, or involuntary labor in any of our operations, and we will not tolerate exploitation of children, physical punishment, or abuse. As part of our commitment to our communities and our world, Honeywell will not tolerate any instances of human trafficking, or other forced labor. We will also never conduct business with any third parties (such as agents or suppliers) who engage in human trafficking or forced labor. Honeywell has adopted the Supplier Code of Conduct that provides clear expectations for suppliers to ensure that they treat their employees with dignity and respect.

For more information, please see our [Human Rights Policy](#)



MAKING POLITICAL AND CHARITABLE CONTRIBUTIONS

Our Company understands the many ways in which the political process enriches our communities. Freedom of belief and conscience are fundamental rights, and we are free to communicate our opinions verbally, in writing, or in graphical form without threat of censorship. However, when we participate in such activities, we should do so on our own time, at our own expense, and ensure that our activities do not conflict with the Code.

We should not use Honeywell property for personal political activities. In addition, we should never engage in any political activities on Honeywell's behalf, unless authorized by the Government Relations function. Never coerce a coworker, especially those with whom you have a reporting relationship, to support your particular causes.

As interested citizens, Honeywell employees are free to make individual personal contributions to candidates of their choice. Employees who are U.S. citizens or who are U.S.-based permanent residents are eligible to participate in the Honeywell International Political Action Committee (HIPAC), provided they meet certain legal requirements. To determine if you are eligible to participate in the HIPAC, contact the Government Relations function, or the general counsel of your business unit.

Lobbying activities are highly regulated. Therefore, we may not make any contacts with government officials in an attempt to influence legislation, regulation, policy, or other governmental actions on Honeywell's behalf without authorization from the Government Relations function. For more information, please see our [Government Relations Policy](#).

Honeywell is committed to social responsibility in every step of the Company's activities. Oftentimes, our Company will support charitable activities in our local communities. Honeywell may engage in such charitable activities, so long as both the charity and the activity have been approved by management, the Law Department, or Honeywell Hometown Solutions.

You may not send emails in an attempt to raise money for an unapproved charity or any other fundraiser on Honeywell's network. In addition, you may not use Honeywell assets, including Company time, for personal charitable pursuits.



INTERNATIONAL TRADE CONTROLS

Honeywell is committed to compliance with all applicable trade laws. This includes import and export control, trade, sanctions and Anti-Boycott laws, as well as regulations in the countries where our Company does business.

Those of us who deal with the importation of goods and export-controlled items, technology, and services have an obligation to understand and comply with applicable regulations. This includes import and export laws, trade sanctions, technology control plans, the conditions, and provisions of export license authorizations that may apply to specific businesses or facilities.

EXPORT CONTROL LAWS

Export control laws govern the transfer of goods, services, and technology from one country to another country. Export controls govern many types of exchanges of technology or technical information across national borders, including email transmissions access to different servers that could contain export controlled technical data, and technical discussions. U.S. export laws and regulations also control the transmission and/or sharing (electronically, orally, or visually) of export-controlled technical data to non-U.S. persons within the United States.

WHAT IF...?

My customer is facing an urgent situation whereby they need Honeywell to send product (hardware, software, or proprietary information) to solve an emergency (e.g., an aircraft on ground situation or a factory that has been rendered offline due to failing controls, etc.) but I do not know the classification. Can I go ahead, and ship given the emergency?

No. You cannot ship product without first confirming the export classification and ascertaining whether an authorization would be required to ship the product. Please contact your Export Compliance Officer for guidance or refer to the [Export Compliance Digital Workplace](#) for more information.

One of my customers has come to me at the end of the quarter with an urgent need for Honeywell product for a project. I am aware that the customer will be supplying the product to another company, but I don't know who. Since I know and trust my customer, do I need to get the end user information?

Yes. Prior to engaging in any transactional activities, you should confirm that all external third parties (vendors, customers, end users, etc.) to the transaction have been screened for third party risks, including trade risks through Honeywell's automated screening tools in our systems. If you are not sure whether screening has happened or the particular transaction is not screened through our systems, you are expected to manually screen all third parties through our screening tools available on the [Sanctions Digital Workplace](#). Please be sure to raise any screening matches or questions to your Export Compliance Officer or to Sanctions Compliance prior to proceeding.

IMPORT CONTROL LAWS

Import laws and regulations govern the importation of goods. Such laws ensure that only admissible goods enter into the importing country, and that the correct amount of duties and taxes are paid on those goods. Honeywell must maintain, among other things, accurate information on the commodity/nomenclature, commercial value, and country of origin of all imported goods.

SANCTIONS LAWS

Trade sanctions laws and regulations govern a wide range of political and/or economic measures that restrict and/or prohibit transactions with specific countries/jurisdictions, entities, industries, individuals, and aircraft/vessels. There is wide variation in the types of sanctions that may apply to a particular transaction, including but not limited to: comprehensive sanctions on a particular country/jurisdiction; selective prohibitions on entities, individuals, and aircraft/vessels; and/or selective restrictions on a transaction's financing or activities. Honeywell must consider trade sanctions implications when engaging in any of its relationships with third parties.

WHAT IF...?

I have done business with a customer for many years. I learned that they are in a country that requires sanctions review. Since we have been working together for years, why is a sanctions review required?

Economic and trade sanctions are long-standing foreign policy tools directed at specific countries, individuals/entities, or activities that a government determines have acted contrary to foreign policy and national security objectives. Because sanctions laws, which impose restrictions and prohibitions on engagement with certain countries and individuals/entities, can change rapidly, it is critical to follow review requirements even for long-standing customers who have never raised issues. Please monitor the list of the countries requiring Sanctions Compliance review on [Sanctions Digital Workplace](#).

ANTI-BOYCOTT

U.S. anti-boycott laws prohibit individuals and entities from participating in a boycott that the U.S. does not support. Antiboycott laws help prevent U.S. companies from being used to implement foreign policies of other nations which run counter to U.S. policy. Honeywell does not cooperate with foreign boycotts that are not approved by the U.S. government. If we receive a request related to any boycott, we must not respond to the request and immediately report the request to Antiboycott@Honeywell.com for disposition, including any reporting required.

For more information on International Trade Controls, please see our

[Export Compliance](#), [Import Compliance](#), and [Sanctions Compliance](#) and [Anti-Boycott](#) policies for more information.

WAIVERS OF OUR CODE

In extremely limited circumstances, Honeywell may find it appropriate to waive a provision of our Code. Approval of any action not compliant with this Code must be sought in advance and may be granted only by the Chief Executive Officer or Senior Vice President & General Counsel of Honeywell. All waivers for members of the Board of Directors or for executive officers of Honeywell require the pre-approval of the Board of Directors and will be promptly disclosed when required by regulation or law. When a waiver is granted, the Board shall ensure that appropriate controls are in place to protect the Company and its shareowners.



Honeywell International Inc.

855 S. Mint Street
Charlotte, NC 28202
www.honeywell.com

Updated August 2024
© 2024 Honeywell International Inc.

