How we win

Our Code of Conduct

Secureworks®

A Message from our CEO

At Secureworks, our purpose is to secure human progress. To fulfill this purpose, our customers, partners, and fellow Secureworks colleagues rely on us to do the right things in the right way. And it is vital that, every day, we uphold the highest standards of individual conduct.

This Code of Conduct is our guidebook. It has the guidance we need to fulfill our promises as Secureworks teammates, and reflects our assurance that we at Secureworks can be relied upon to make the right decisions.

I appreciate you taking the time to read and follow this Code of Conduct. And thank you for making Secureworks a great place to work, where we seek to improve the lives and prosperity of all whom we serve.

– Wendy Thomas

Contents

Introduction

Secureworks' Code of Conduct is our guidebook for winning with integrity.

About our Code of Conduct

Our Code applies to all of us

Our Code of Conduct, "How We Win," provides general guidance on how to carry out our daily activities in accordance with our values, as well as in compliance with the letter and spirit of applicable legal requirements and Secureworks policies, standards and ethical principles. All Secureworks team members, including officers and directors, must follow our Code. We also expect all our suppliers, assigned workers, agents and others doing business with Secureworks or acting on our behalf to hold themselves to equally high standards.

Our Code is a global Code

Secureworks is a U.S.-based company, proudly employing team members and serving clients all over the world. We comply with the laws of the U.S. and other countries where we do business. Our Code of Conduct applies to all Secureworks team members globally. While we embrace diversity and respect cultural differences, if a local custom or business practice violates our Code, we must follow the Code. If something permitted or required by our Code violates local law, we must follow local law. In those rare circumstances where it appears that local law may conflict with U.S. law, contact the Legal Department or the Global Ethics & Compliance Office for guidance.

Refer to the Code and ask questions

Please read the Code and refer to it often. It isn't something you read one time and forget about. It's your guidebook for winning with integrity. To supplement the general guidance of the Code, Secureworks may adopt more specific policies and standards that apply globally, geographically or to certain business units, functions or departments. Team members and leaders are expected to abide by the Code, Secureworks policies and standards. Failure to do so may result in disciplinary action, up to and including termination, where allowed by law. Familiarize yourself with the Code and the laws, policies and standards that apply to you in your role at Secureworks. You must also take all required ethics and compliance courses in a thoughtful and timely manner. Of course, our Code and policies can't address every possible situation, so it is up to you to use good judgment and seek help whenever you have questions or aren't sure about the right course of action. Review the FAQs and other helpful resources on the Global Ethics & Compliance intranet site. Talk to your leader or contact Human Resources, the Legal Department or the Global Ethics & Compliance Office if you still have questions.

Speak up, report concerns

If you suspect that someone is behaving illegally or unethically, please speak up. Talk to your leader, call the Ethics Helpline, submit an online report via the web-based EthicsPoint, send an email to ethics@secureworks.com or use any of the other resources and reporting avenues described in the Code or on the Global Ethics & Compliance intranet site. Secureworks does not tolerate retaliation against anyone who, in good faith initiates or participates in the Ethics process, asks questions or raises concerns.

Team members and leaders are required to cooperate in Company investigations and follow the instruction of Legal, HR and Global Ethics & Compliance during such investigations.

Approval, amendments and waivers

Our Code has been approved by the Secureworks' Board of Directors. Any substantive amendments to the Code must be approved by the Board or an appropriate Board committee. A request for a waiver of a

provision of our Code for any Secureworks executive officer or Board member must be submitted to the Global Ethics & Compliance Office and approved by our Board of Directors. If approved, Secureworks will publicly disclose the waiver and the reasons it was granted.

Make a commitment

As Secureworks team members, we all need to show our commitment to winning with integrity by acknowledging that we've read, understand and agree to abide by the Code. We are required to do this when we are hired and to renew this commitment annually. Because integrity is so important to our long-term success, failing to abide by the Code can lead to disciplinary action up to and including termination of employment. Please note, though, that the Code is not a contract of employment, and Secureworks may interpret, modify or rescind some or all of the Code provisions, as well as related policies and standards, at any time.

Secureworks' ethical principles

We do the right thing

Sometimes, the world influences us to start thinking something that is wrong isn't "that" wrong or that it might be a little easier to do the "almost-right" thing. Don't get pulled into that kind of thinking. Stand up and speak up for what is right.

We are honest

What we say is true and forthcoming—not just technically correct. We are open and transparent in our communications with each other and about our business performance.

We are trustworthy

Our word is good. We keep our commitments to each other and to our stakeholders. We do the right thing without compromise. We avoid even the appearance of impropriety.

We treat others with respect

We value their contributions and listen to their point of view. We maintain fairness in all relationships.

We are courageous

We speak up for what is right. We report wrongdoing when we see it.

We use good judgment

We think before we act. We use our purpose, values and ethical principles as decision filters to guide our behavior.

We are responsible

We accept the consequences of our actions. We admit our mistakes and quickly correct them. We don't retaliate against those who try to do the right thing by asking questions or raising concerns.

Always obey the law and Secureworks' policies

But that's just the minimum. Strive to live up to our values and ethical principles as well.

Never compromise on integrity

Turn down business if you can't do it legally and ethically. Don't let pressure to succeed make you do things you know are wrong.

Just say no

It's not only OK to refuse to follow directions that you know are illegal or unethical, it's required. No Secureworks manager has the authority to make you violate the law, our Code, policies or ethical principles.

Make good choices

Use our values and ethical principles as decision filters. When you aren't sure of the right course, ask for help.

Select business partners carefully

Choose those who share our values and high standards for legal and ethical business practices. Don't let anyone damage our reputation and our brand by acting illegally or unethically in Secureworks' name.

Speak up

If you suspect someone —a team member, leader, business partner or client—is acting illegally or unethically, help us maintain our values and culture by reporting it immediately.

If you ever have concerns about your own behavior, speak up about that as well. Admitting mistakes and taking action to correct them is the responsible thing to do.

Be a force for good. Take pride in our values and culture and show others how you feel.

If you're ever unsure of what to do, ask yourself these questions.

If the answer to any of them is "no," don't do it. If you are still unsure, seek help.

Additional responsibilities for managers

If you are a Secureworks manager, you have a special responsibility to lead with integrity. It is not enough for you to behave legally and ethically yourself. You must also take affirmative steps to influence your team members to do the same. This requires a visible commitment to promote ethical conduct and compliance with legal requirements, our Code and Secureworks policies. This means you must:

- Be a positive role model. We all know actions speak louder than words, so let your actions demonstrate your belief that business goals and profits never trump compliance with legal requirements and ethical principles.
- Inspire winning with integrity. Set the right tone from the top. Be comfortable talking with your team members about the importance of acting legally and ethically. Explain how our Code supports our mission and values and ensures our success.
- Thoughtfully complete your own ethics and compliance training in a timely manner, and make sure your team members do the same.
- Become familiar with the Code and the laws and policies that apply to your organization. Adopt and follow compliance processes designed to prevent violations.
- Celebrate achievement. Recognize and reward team members whose behavior exemplifies our value of winning with integrity.
- Create an environment where team members know they can ask questions or raise concerns without fear of reprisal. Be available to answer your team members' questions and address their concerns. Never retaliate against anyone who reports a good faith concern or cooperates with internal investigations or audits. And don't tolerate others who do.
- Understand your special obligation to report behavior that you know—or should know—is illegal or violates Secureworks' policies or ethical principles. Respond swiftly and appropriately to misconduct.

Our commitment to our people

Secureworks doesn't achieve our goals, our people do. All Secureworks team members are connected by our mission and values; our relationships with each other are what drive Secureworks' success. We honor and nurture those relationships by seeking out and welcoming diversity, being open and honest in our interactions, and creating an environment of collaboration and inclusion. We treat everyone with dignity and respect, and comply with all laws relating to employment rights and working conditions in the countries where our team members live and work.

Raising issues and concerns

What we believe

Team members must be able to ask questions and raise issues without fear of retaliation, secure in the knowledge that their concern will be treated seriously, fairly and promptly.

What it means for you

Promptly raise ethics and compliance questions and immediately report suspected unethical, illegal or suspicious behavior. SecureWorks does not tolerate retaliation against anyone who makes a good faith report of suspected misconduct or otherwise assists with an investigation or audit.

There are many ways to ask questions or raise concerns and you should use the method you prefer: talk with your manager or a member of management; contact Human Resources, the Legal Department or the Global Ethics & Compliance Office; or access Secureworks' third-party Ethics Helpline via telephone or online via the EthicsPoint to report your concern confidentially or anonymously, where the law allows.

Note: In situations involving imminent threat of personal harm, you should immediately notify Secureworks Security, law enforcement or other emergency services as appropriate under the circumstances.

Did you know . . .

Secureworks' telephone-based Ethics Helpline and web-based Ethicsline are available 24 hours a day, 7 days a week, 365 days a year. All reports of ethics and compliance concerns are treated confidentially. Reports may also be made anonymously where the law allows.

Investigating and addressing concerns

What we believe

Our commitment to winning with integrity requires that we take all credible good faith reports of suspected misconduct seriously, investigate them fairly and confidentially, and take appropriate corrective action where warranted.

What it means for you

The Global Ethics & Compliance Office is responsible for overseeing all internal investigations of suspected ethics and compliance-related misconduct, including violations of law, or our Code of Conduct and related policies.

The Global Ethics & Compliance Office has established processes and procedures to ensure that all internal investigations are conducted by qualified personnel who have been trained to conduct investigations lawfully, promptly, thoroughly, professionally, fairly and confidentially.

Team members and managers should not interfere in internal investigations or engage in their own fact-finding. Rather, you should promptly raise ethics and compliance questions and immediately report suspicious behavior.

Team members and others involved in internal investigations will be treated with dignity and respect. All investigations and any resulting corrective action will be conducted in compliance with local law, applicable Secureworks policies and any required workers' representative consultation requirements.

All team members are expected to cooperate in internal investigations, audits, accounting reviews or directions from Secureworks' lawyers in connection with lawsuits or government investigative proceedings. Searches of company-provided physical and information technology resources may be required.

Retaliation will not be tolerated against any team member who cooperates in these kinds of company activities.

After an investigation is completed, appropriate disciplinary and other corrective action will be taken when warranted by the facts. Secureworks may, in appropriate cases and subject to applicable local law, notify government authorities and cooperate with any resulting prosecution or other government action.

In addition, when legally required or otherwise appropriate, Secureworks will timely self-report compliance violations to applicable government authorities and cooperate with any resulting official proceedings. The determination of whether and when to refer a matter to government authorities, or to self-report compliance violations, will be made by Secureworks' General Counsel or his or her designees.

If you think you are being retaliated against, or that an investigation is being conducted inappropriately, you should report it immediately using any of the reporting avenues available to you.

Q&A

I reported misconduct through the Ethics Helpline but never heard about an investigation or other action.

If you made your report anonymously, the investigator may not have been able to get in touch with you. Even if the investigator was able to reach you, he or she may not have been able to share the outcome because of privacy and confidentiality concerns. In any case, you should not hesitate to follow up—call back to the Helpline and ask whether the matter has been resolved.

Diversity, equal opportunity and respect

What we believe

Having a diverse workforce—made up of team members who bring a wide variety of skills, abilities, experiences and perspectives—is essential to our success. We are committed to the principles of equal employment opportunity, inclusion and respect.

What it means for you

All employment-related decisions must be based on company needs, job requirements and individual qualifications. Always take full advantage of what our team members have to offer; listen and be inclusive.

Never discriminate against anyone—team members, clients, business partners or other stakeholders—on the basis of race, color, religion, national origin, sex (including pregnancy), age, disability, HIV status, sexual orientation, gender identity, marital status, past or present military service or any other status protected by the laws or regulations in the locations where we operate.

Comply with laws regarding employment of immigrants and non-citizens. Provide equal employment opportunity to everyone who is legally authorized to work in the applicable country.

Provide reasonable accommodations to individuals with disabilities and remove any artificial barriers to success.

Report suspected discrimination right away and never retaliate against anyone who raises a good faith belief that unlawful discrimination has occurred.

Q&A

I recently applied for a job in another department and believe I was not selected because I'm a woman. What should I do?

Use any of the available reporting avenues to share your concerns immediately. Secureworks requires that employment decisions be made without regard to a person's sex (gender).

Compensating team members fairly and lawfully

What we believe

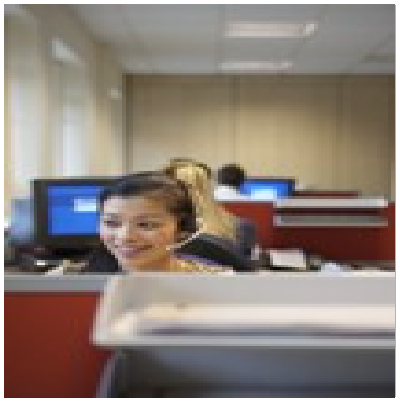
Our team members devote their time, talents and energy to fulfilling our mission and they deserve to be compensated fairly for their efforts. We comply with all applicable laws concerning pay, benefits and working conditions.

What it means for you

Laws relating to pay, employment benefits, hours of work, time off, leaves of absence and other terms and conditions of employment vary from country to country, and team members are expected to comply with all applicable employment-related laws. Immediately report any suspected violation of law or policy.

Managers must ensure that their team members are paid timely, accurately and in accordance with applicable legal requirements and Secureworks policies. Understand the activities that must be recorded and reported as time worked and never instruct team members to omit covered activities in their time records. Do not withhold or deduct any amount from a team member's pay except as required or permitted by law.

Team members who are required to record and report their time worked must do so accurately and completely. Never over or understate your time worked or otherwise provide incorrect or inaccurate time records. Failing to do so—by over-reporting or under-reporting time worked—can lead to disciplinary action up to and including termination.



Preventing harassment

What we believe

All Secureworks team members should be able to do their jobs in a safe and respectful environment without fear of harassment.

What it means for you

Always treat everyone—team members, clients, business partners and other stakeholders—with dignity and respect.

Understand that harassment includes actions, language, written materials or objects that are directed or used in a way that undermines or interferes with a person's work performance, or creates an intimidating, hostile or offensive work environment.

Never target anyone for negative treatment on the basis of race, color, religion, national origin, sex (including pregnancy), age, disability, HIV status, sexual orientation, gender identity, marital status, past or present military service or any other status protected by the laws or regulations in the locations where we operate.

Be aware that all forms of harassing conduct are prohibited at Secureworks, including unwanted sexual advances, invitations or comments; visual displays such as derogatory or sexually-oriented pictures or gestures; physical conduct including assault or unwanted touching; or threats or demands to submit to sexual requests as a condition of employment or to avoid negative consequences.

Harassing conduct will not be tolerated. If you see harassing conduct, speak up. In minor cases, first tell the person to stop and if it continues, report it right away. In serious cases, go straight to a leader, Human Resources or the Global Ethics & Compliance Office.

Never retaliate against anyone who raises a good faith belief that unlawful harassment has occurred.

Did you know . . .

Our policy against harassment is broader than the legal definition and prohibits all behavior that undermines or interferes with a team member's work performance by creating an intimidating, hostile or offensive work environment.

Ensuring a non-violent workplace

What we believe

A workplace free of violence, weapons and other disruptive behavior keeps team members safe and able to concentrate fully on their jobs.

What it means for you

Be polite and respectful at all times. If you disagree with a team member or other person at work, try to resolve it calmly. Never bully, threaten, intimidate or harm another person or their property through either verbal behavior (written or oral) or non-verbal behavior (such as gestures or expressions).

Unless authorized by law or Secureworks policy, you may not possess, conceal or use weapons, including firearms, knives, clubs, ammunition, explosives or other devices that are primarily used to inflict injury (including recreational weapons such as hunting rifles or crossbows) while on company property or when conducting Secureworks business. This prohibition does not apply to knives or other tools which are required, permitted or provided by Secureworks as part of a team member's job assignment.

This policy applies to anyone who enters Secureworks property, which includes buildings, parking lots, walkways and any other property we own, lease or occupy. If weapons are discovered in violation of this policy, they will be confiscated, where permitted by local law.

Did you know . . .

Our prohibition against weapons does not apply to law enforcement or company security officers, government or military authorities or their agents acting in an official capacity or others who are authorized to carry weapons on company property.

Maintaining a drug-free and alcohol-free workplace

What we believe

Alcohol, illegal drugs and controlled substances can adversely affect safety, productivity, attitude, reliability and judgment. They have no place in the workplace.

What it means for you

With the exception of lawful, moderate and prudent alcohol consumption during legitimate business entertainment, team members are prohibited from consuming or being under the influence of alcohol, or possessing, distributing or being under the influence of illegal drugs while working or engaging in Secureworks business on or off company property.

We are committed to a drug-free and alcohol-free workplace. As part of that commitment, we take all appropriate and legally required steps to ensure compliance, which may include testing of job applicants or requiring disclosure of criminal alcohol and drug statute convictions.

Q&A

I'll be attending a trade show on Secureworks' behalf and they will be serving alcohol at the opening reception. Is it OK to drink alcohol at the reception?

Yes, provided you are legally entitled to drink alcohol under applicable law and do not drink to excess or become impaired. Don't embarrass yourself or Secureworks by your behavior.

Did you know . . .

"Illegal drugs" and "controlled substances" include prescription drugs being used illegally.

Respecting the privacy of team member's personal information

What we believe

Each of us has a responsibility to safeguard the confidentiality, integrity and security of team member's personal information. We comply with all applicable privacy and data protection laws in the countries where we operate.

What it means for you

Secureworks may collect personal information about team members to meet legal requirements or enable effective business operations.

If your role requires that you have access to team member personal information, make sure you take steps to properly secure it, and that you access or use it only when authorized by Secureworks for legitimate business needs and in accordance with applicable laws and Secureworks policies.

Regardless of your role, if you gain access to a team member's personal information or other private data, always take care to keep it secure and never share it with anyone—inside or outside of Secureworks—without the team member's permission except as necessary to meet legal or legitimate business requirements.

See the Code provisions on Protecting customer personal data and privacy for a description of what constitutes personal information and additional guidance.

For additional information, please consult the applicable Secureworks policies and standards.

Did you know . . .

It is a criminal offence in some countries to misuse personal information. There are many laws relating to the privacy of personal information. Even where there are no laws, Secureworks' Data Privacy Policy requires that you properly collect, handle and secure personal information.

Communicating responsibly

What we believe

Our communications help us connect with each other, our clients and other stakeholders. What we say reflects who we are and what we stand for. We should always communicate in ways that demonstrate our values, further our purpose and enhance our reputation and brand.

What it means for you

Be careful how you talk to others—especially in any form of written communication, which includes electronic and online communications such as email, instant messaging, online chats, blogs or posts on social networking sites.

Be objective and professional. Avoid offensive, inflammatory or aggressive language, as well as anything that would embarrass or disparage Secureworks.

Be truthful and accurate. Misstatements—even if inadvertent—can put you and Secureworks at serious risk. Do not exaggerate, make broad generalizations, speculate about matters with legal significance or make statements that could be taken out of context.

Did you know . . .

Information you share through instant messaging, texts, blogs and social networking sites (such as Facebook, Twitter, Yammer, etc.) can be far-reaching, permanent and have a negative or damaging impact on you, Secureworks and our stakeholders.

Tailor the scope and content of your communications appropriately. Do not send emails to people who do not have a legitimate need to receive them. Use large distribution lists sparingly and put them in the Bcc address field. Use "reply all" prudently. Only post information on public forums or social networking sites that is appropriate for a wide audience. Be concise and do not include unnecessary information or details.

Unless explicitly authorized to speak on behalf of Secureworks, you must make it clear that your personal views are yours alone and do not reflect Secureworks' views or represent an official company position.

Be careful not to disclose confidential information belonging to Secureworks or others except to those who have a legitimate need to know and who are authorized to access the information.

Q&A

Sometimes I talk about things that happen at work on my personal blog—is that a problem?

It depends. Remember, you are personally responsible for Secureworks-related content you publish online. Always think before you post or send and follow the rules for careful communications.

Workplace health and safety

What we believe

We conduct business in accordance with applicable health and safety requirements and strive for continuous improvement in this regard. No one should ever become ill or injured as a result of their work for Secureworks.

What it means for you

Team members are expected to perform their work in compliance with the health and safety laws, regulations, policies and procedures of their locations. Always use caution and apply safe work practices when you are working in remote locations or at home.

Team members working at client locations must also follow the client's health and safety requirements.

Communicate applicable safety and health requirements to anyone coming onto a Secureworks site, including visitors, clients, assigned workers and contractors.

Immediately report workplace injuries, illnesses or unsafe conditions including "near-misses." Timely reporting may help prevent others from being injured.

Q&A

My manager has suggested adopting a practice that will save time but poses a potential safety risk. What should I do?

Never compromise your safety or the safety of your team members or others. Report the matter to another manager or use the other available reporting avenues.

Our commitment to our shareholders

We are committed to growing the value we bring to our shareholders, honoring their trust and safeguarding their investment. We will comply with all applicable legal requirements and stock exchange rules relating to corporate organization and governance, securities registration and trading, business licenses and taxes, and authorization to do business.

Integrity of financial statements and regulatory filings

What we believe

The integrity of our financial statements and other regulatory filings is critical to the successful operation of our business, and to maintaining the confidence and trust of our shareholders, clients, business partners and other stakeholders.

What it means for you

All financial information about Secureworks filed with the U.S. Securities and Exchange Commission or disclosed publicly, as well as all information in statutory financial statements and tax filings must be accurate and complete, and must comply with applicable accounting principles and legal requirements.

If you are involved in Secureworks' financial reporting process, make sure that all transactions and balances are timely and accurately recorded, classified and summarized in accordance with Secureworks' financial and accounting practices.

Did you know . . .

Even if you are not in a finance or accounting role, you still have responsibilities relating to the integrity of Secureworks' financial statements. Everyday transactions such as recording expense reports and preparing sales invoices feed into our financial statements and must be accurate and complete. Likewise, you should be candid and forthcoming in making forecasts and outlooks.

Never misrepresent our financial or operational performance or otherwise knowingly compromise the integrity of the company's financial statements. Do not enter information in the company's books or records that intentionally hides, misleads or disguises the true nature of any financial or non-financial transaction, result or balance.

Follow all processes and controls designed to ensure the accuracy of Secureworks' assessment and reporting of its financial results. If you are responsible for overseeing, operating or evaluating Secureworks' internal controls over financial reporting, make sure you perform your duties in accordance with Secureworks policies, guidance and instruction. If you are asked to provide, review or certify information related to Secureworks' internal controls, provide the information requested and otherwise respond in a full, accurate and timely manner.

Be sure to retain, protect and dispose of company financial records in accordance with applicable legal requirements and Secureworks record retention policies.

Always cooperate and communicate openly with members of Secureworks' internal audit, accounting, ethics and compliance, and legal teams, as well as with Secureworks' independent auditors and government investigators or regulators with respect to Secureworks' accounting practices or financial statements. Never attempt to influence, coerce, manipulate or mislead any of them. If a government investigator or regulator asks you to take part in an investigation, notify the Legal Department or the Global Ethics & Compliance Office immediately to ensure Secureworks can respond in a timely, organized and coordinated manner.

Q&A

I believe a team member made a false statement to Secureworks' independent auditor. What should I do?

Report the matter immediately to the Legal Department or CISO Team, or you may also notify the company at AskHR@secureworks.com.

Avoiding conflicts of interest

What we believe

We are loyal to Secureworks and always act in the company's best interests. We avoid conflicts of interest, or even the appearance of a conflict, as well as other activities that could harm or reflect negatively on Secureworks.

What it means for you

A conflict of interest can occur when our personal activities, investments or associations compromise our judgment or ability to act in Secureworks' best interests. Secureworks team members need to understand and avoid the types of situations that can give rise to conflicts of interest. To help protect Secureworks's interests, always disclose any of your relationships, associations or activities that could create actual or potential conflicts of interest to your manager, Human Resources or the Global Ethics & Compliance Office so the situation can be evaluated and addressed appropriately.

Personal relationships

If one of your family members or someone with whom you have a significant personal relationship also works at Secureworks, make sure that all your actions and decisions are made in Secureworks' best interests, and not because of your personal or family relationships. You should not be involved in any employment-related decisions—such has hiring, compensation, evaluation or promotion—regarding a family member or someone with whom you have a close personal relationship.

Did you know . . .

Just as your actions at Secureworks should not benefit your personal business or financial interests, they also should not benefit the business or financial interests of your family members or others with whom you have a significant personal, business or financial relationship.

Outside employment, business ventures and investments

All Secureworks team members need to be sure that their secondary employment, outside business ventures or other commercial or financial activities do not take away from their responsibilities to Secureworks. Do not use Secureworks equipment or resources (including confidential information or intellectual property, or that of our clients and other third parties) in connection with these outside activities, and ensure they don't jeopardize your productivity or ability to perform your duties for Secureworks. Never engage in any outside employment or other activity that competes with Secureworks, violates your confidentiality or other obligations to Secureworks, or that is illegal, immoral or would otherwise reflect negatively on Secureworks.

Always select vendors and business partners who will serve SecureWorks' best interests. To avoid actual or perceived conflicts of interest, you should not participate in any decisions relating to current or potential business relationships between Secureworks and your secondary employer, personal business ventures or entities in which you have a significant financial investment or serve in a governance position. Likewise, you should refrain from using information about business opportunities learned in your role at Secureworks for your own or anyone else's benefit except as allowed by law and applicable Secureworks policy.

Outside board memberships and governance roles

All Secureworks team members owe a duty of loyalty to Secureworks and are expected to devote their principal efforts to Secureworks business. In addition, outside board service with a for-profit company (whether publicly traded or private) can present conflicts of interest and other issues. As a result, non-Executive Secureworks team members are not permitted to serve on the boards of outside for-profit companies, whether publicly traded or private. Secureworks Executives are not permitted to serve on the boards of outside for-profit companies, whether publicly traded or private, except in strict adherence to SecureWorks' Outside Board Membership Policy and with the approval of Secureworks' Chief Executive Officer and the Secureworks' Board of Directors.

Service on the board of a non-profit entity is generally permitted but must also adhere to Secureworks' Outside Board Membership Policy.

The Global Ethics and Compliance Office administers Secureworks' Outside Board Membership Policy and should be consulted on any questions concerning that policy and must be your first stop if you wish to serve on an outside for-profit board.

Industry associations and advisory committees

Secureworks may ask you to serve on its behalf in industry or trade associations, on standards-setting bodies, client or supplier advisory boards or similar organizations. In those situations, you are a representative of Secureworks and must ensure you are always acting in Secureworks' best interests. Don't make commitments on behalf of Secureworks unless you have the authority to do so.

You may participate with these kinds of organizations in your personal capacity if approved by a Secureworks leader at the vice president level or above, and provided you make it clear that you are not acting on Secureworks' behalf and your participation does not conflict with SecureWorks' interests or reflect negatively on Secureworks.

Q&A

I have been asked to participate as a subject-matter expert for a paid research network. Is that allowed?

No. Secureworks will not permit current team members to participate in that type of paid outside engagement, as there is too much opportunity for Secureworks confidential information to pass between parties. To ensure this is avoided, team members wishing to engage in outside consulting activities should seek permission through the Legal Department or CISO Team, to ensure that these opportunities are permissible.

Avoiding insider trading

What we believe

Secureworks takes its responsibilities under the U.S. Federal Securities laws very seriously, and expects team members to do the same. You should never use or disclose material non-public information prior to its official public release.

What it means for you

"Material non-public information" about a company is information that a reasonable shareholder would consider important in making a decision to buy or sell stock. Examples may include yet-to-be-announced financial information, mergers or acquisitions, supplier or client relationships, changes in leadership team management and new solutions.

Insider trading occurs when an individual with knowledge of material non-public information about a company uses it to gain profits or avoid losses in the stock market.

As a Secureworks team member, you may have access to "inside" information about our company or other companies such as current or potential suppliers, clients or acquisition targets. You are obligated to keep this information confidential and you, your family members and individuals with whom you have a significant personal relationship must never use this kind of information to trade in any company's securities.

Likewise, you must never provide stock tips or share inside information with any other person who might use it to trade stock. Even if you don't intend for someone to act on the information, sharing it would violate your confidentiality obligations to Secureworks and could result in accusations of insider trading against you or Secureworks.

Q&A

I heard from one of my team members that Secureworks is planning to acquire a publicly-traded company, but it hasn't been announced yet. Can I suggest to my friends that they buy stock in that company?

No. Not only would this violate your confidentiality obligations to Secureworks, you could be charged with illegal insider trading.

Did you know . . .

Secureworks has policies that prohibit team members from engaging in certain kinds of transactions involving Secureworks stock such as derivatives, puts and calls, and short selling. All team members should be aware of and comply with these policies.

Preventing theft and fraud

What we believe

Theft and fraud are crimes and will not be tolerated. When team members steal or commit fraud, it damages our reputation and brand and hurts us all.

What it means for you

We all know what theft is: it's taking something that doesn't belong to you without permission. It can include physically taking something like money or property, or it can be done through other means like forgery, embezzlement and fraud.

Fraud is a type of theft by deception. It involves making someone believe (by words or conduct or by concealing important information) something that isn't true, with the intent of having them take (or refrain from taking) some action in reliance on the misrepresentation with the result that they suffer economic harm.

Any team member who engages in or assists others with theft or fraud will be subject to disciplinary action up to and including termination and will also be subject to prosecution.

Help safeguard Secureworks' assets and reputation by watching for any kind of fraudulent activities against SecureWorks, our team members, clients, shareholders, business partners or other stakeholders. Always report suspicious activity immediately.

Giving and accepting gifts and entertainment

What we believe

We are committed to winning business only on the merits and integrity of our solutions, services and people. Likewise, our business decisions should always be made in the best interests of Secureworks. We comply with all legal requirements pertaining to giving and receiving gifts and entertainment.

What it means for you

Gift giving and entertaining among business partners can be appropriate ways to show appreciation, develop deeper understanding and build goodwill. But it can also create the perception that business decisions are made because of these benefits and not on the basis of fair and objective criteria. The legal requirements relating to business gifts and entertainment are complex, and Secureworks team members need to use sound judgment, comply with the law, and never allow gifts, entertainment or other personal benefits to influence our decisions or undermine the integrity of our business relationships.

Accepting gifts

Team members should never solicit or accept tangible or intangible personal benefits of any kind that are given—expressly or implied—in exchange for securing Secureworks business or providing favorable business terms, or that might create or give the appearance of creating a sense of obligation on your part with regard to the giver. Never accept gifts or entertainment that are illegal, immoral or would reflect negatively on Secureworks.

Except as described above, you may accept occasional unsolicited personal gifts of nominal value such as promotional or commemorative items. You may never accept gifts of cash, cash equivalents, stock or other securities. Gifts that are intended to benefit Secureworks rather than you personally may be of greater than nominal value but they must be turned over to Secureworks for appropriate disposition.

All business meals and entertainment must be customary, unsolicited, infrequent, in good taste, reasonable in value and

provided for legitimate business reasons as described above. If the provider of the meal or entertainment is not in attendance, it is considered a gift and can only be of nominal value.

You should politely decline gifts or entertainment that do not comply with this or more restrictive policies. If that would be difficult or embarrassing to the giver, ask your manager or contact the Legal Department or CISO Team for guidance.

Giving gifts

Many of the same general concepts and precautions relating to accepting gifts and entertainment also apply when providing gifts or entertainment to employees of commercial businesses. Any such benefits must be for legitimate business purposes, reasonable in amount, in good taste, not in the form of cash, cash equivalents or securities, and must never be given in exchange for securing business, providing favorable business terms or other business activity. You must also comply with the gift and entertainment policies of the recipient's organization.

The rules relating to doing business with government entities and their employees are much more strict and complex. Team members must always comply with legal requirements and government rules relating to gifts, entertainment or other personal benefits provided to government employees or officials.

When dealing with non-U.S. governments, always comply with local legal requirements and follow our policy on the Foreign Corrupt Practices Act, which applies to all SecureWorks team members around the world.

When dealing with U.S.-based federal, state and local governmental entities and other public institutions, always comply with applicable laws, regulations and Secureworks policies. In particular, you must never use Secureworks funds to give anything of value to U.S. Congressional officials, members of the U.S. Senate or House of Representatives or any of their staffs. Even personal gift-giving to these individuals is restricted. Please refer to Dell's policy on giving gifts to U.S. congressional officials for additional guidance. If you have questions about giving gifts to government clients or their employees, ask your manager or contact the Legal Department or the Global Ethics & Compliance Office.

Always promptly and accurately report gift and entertainment-related expenses, regardless of whether the recipient is a commercial or public entity, and even if the gift or entertainment may be contrary to applicable law, Secureworks', Dell's or the recipient's policies.

Q&A

A new vendor is grateful for the work I did to expedite execution of their Secureworks contract and sent me a bottle of champagne valued at US$40. It's OK to accept it since it's not very expensive, right?

No. Even if the value is below the dollar limit established in the policy that applies to you, you may not accept it because it was offered in exchange for your actions related to their business with Secureworks. You should return the gift to the vendor and tell your manager about it.

Did you know . . .

You should always check the global, regional or Secureworks policies that apply to you; they may specify more restrictive requirements on giving or accepting gifts and entertainment which must be followed.

Using information technology and other resources

What we believe

Secure and reliable information technology resources are essential to the operation of our business. We have a responsibility to comply with proper safeguards and abide by Secureworks policy at all times when using these and other Secureworks resources.

What it means for you

Secureworks provides team members with facilities, furniture, supplies, equipment and information technology resources to help them perform their work for Secureworks. We must all be good stewards of these resources. We need to use and maintain them carefully and protect them from theft, loss, damage, waste and abuse.

Team members may occasionally use Secureworks resources, including information technology resources, for limited personal use, but it must be appropriate and kept to a minimum. Inappropriate use would include such things as engaging in illegal activity, viewing pornography, accessing hate sites and hacking. Team members also should never use Secureworks' resources to support secondary employment, outside business ventures or personal political activities.

Consistent with local laws, Secureworks reserves the right to monitor the use of its resources, including its information technology resources. Where permitted by local law, your use of the resources constitutes consent to such monitoring.

Help keep our physical assets safe and secure by following all security rules and procedures such as using your badge when entering facilities and securing valuable equipment like notebook computers.

Help keep our information technology resources safe from viruses, malicious software programs and intrusion attempts by following all information security policies. Don't install unauthorized software, applications, hardware or storage devices on your Secureworks-issued computer or other device, and don't access Secureworks' network via unauthorized applications or devices.

Create a strong password in accordance with Secureworks policy and do not share it with anyone. Remember you are responsible for all activity performed with your individually assigned user ID.

Make all internal computer equipment requests through Secureworks Identity Now (Identity Manager) system and SNOW (Service Now) ticketing system. Only download approved software and applications via the Secureworks software download portal.

Team members with access to client information technology resources should follow the client's policies and procedures relating to use of information technology resources and information security.

Did you know . . .

Information technology resources include all types of communication and computing equipment and devices; access to Internet and intranet; networking capabilities; and software programs and applications.

Effective information lifecycle management

What we believe

Secureworks information is an important asset and managing it appropriately can be a competitive advantage for Secureworks. Each of us is responsible for the appropriate protection, management and disposition of Secureworks information in accordance with applicable law and Secureworks policies and standards available via the Ethics and Compliance portal on the Secureworks Intranet.

Effective information management helps Secureworks continue to earn the trust of its clients to handle their information.

What it means for you

You are required to adhere to Secureworks' information lifecycle management policies and standards. Certain Secureworks business, transactional and other information must be retained for a period of time. Retain all such Secureworks information in accordance with applicable retention requirements and store it in approved electronic or physical storage locations.

Properly dispose of all Secureworks information that is no longer needed for business operations and has satisfied its retention requirements as long as the information is not subject to a preservation directive ("Legal Hold") from the Legal Department. A "Legal Hold" is a written or oral directive from Secureworks' Legal Department advising a Secureworks team member that certain information relevant to a Secureworks legal matter must be saved until further notice from the Legal Department. You must always comply with the directions in a Legal Hold. Do not dispose of any Secureworks information that is subject to a Legal Hold until you are authorized by the Legal Department to do so.

For additional information, please consult the applicable Secureworks policies and standards.

Did you know . . .

One of the core principles of effective information lifecycle management is sharing information on a "need-to-know" basis only. Be mindful of whether everyone in your "addressee list" needs to be copied on your email. In addition, consider whether you are sharing too much information for the transaction at hand. Even if an individual has a need-to-know, be careful about how much information needs to be shared at that time. Effective lifecycle management begins with you and means practicing thoughtful information sharing all the time.

Safeguarding our other confidential information

What we believe

Secureworks confidential information, including intellectual property like trade secrets, is a tremendously valuable asset that differentiates us from our competitors and must be protected. Every Secureworks team member is responsible for the appropriate protection of these important assets.

What it means for you

"Confidential information" is a term used to describe important or valuable business information belonging to Secureworks that is not generally available to the public. It includes patents, trade secrets, copyrights and other intellectual property that have been developed, licensed or acquired by Secureworks. It can also include information belonging to or about clients, business associates or others stakeholders that has been disclosed to Secureworks under obligations of confidentiality.

Examples include unannounced financial information, strategic business plans, unannounced product or services and solutions offerings, planned or contemplated mergers or acquisitions, lawsuits and other legal proceedings, product design and technical knowledge, and client and team member personal information.

Always be careful to protect confidential information belonging to Secureworks, as well as confidential information belonging to our clients, business associates and other stakeholders. Take reasonable physical and electronic precautions to safeguard the information.

Label confidential information appropriately and in accordance with Secureworks policies and standards. Don't view or work with confidential information in a non-secure setting. Don't leave hard copy confidential information out in the open—lock it up when you aren't using it. Keep a clean and secure workspace, wherever you are working, especially if you are working outside of a secure Secureworks facility.

Store electronic confidential information only in secure locations or on secure devices, limit access and appropriately use encryption technology. Dispose of confidential information securely—shred hard copy documents and use secure and effective methods for deleting electronic information in accordance with Secureworks policies and standards..

Unless secured by means provided or approved by the Information Technology Department, do not access or store Secureworks confidential information on non-Secureworks-issued devices such as your personal smart phone, laptop, desktop or other computing device.

Share confidential information only with individuals – whether team members or other stakeholders - who have a legitimate business need to know. Share only as much information as is needed – do not overshare. Share confidential information only with third parties who are covered by contractual non-disclosure agreements or when there are similar protections in place. Some confidential information is highly sensitive and even internal knowledge and access is restricted. Therefore, you may be required to sign an internal non-disclosure agreement and be restricted from sharing or discussing the confidential information with other team members unless they have also signed an internal non-disclosure agreement.

Always be very careful when talking about confidential information. Avoid discussing confidential information in public places,whenever possible, and never share it family members and friends. If you must discuss or handle confidential information in a public setting, take extra precautions against an unintended disclosure.

Remember that Secureworks' confidential information belongs to Secureworks and that you may not use it for personal gain. If you develop intellectual property in your job or while employed by Secureworks, you must disclose it to Secureworks because the rights to that property may legally belong to Secureworks. You are prohibited from the unauthorized disclosure, duplication or distribution of Secureworks confidential information, including intellectual property belonging or entrusted to Secureworks.

Even if you leave Secureworks, you are still legally and contractually obligated to maintain the confidentiality of Secureworks' information.

For additional information, please consult the applicable Secureworks policies and standards.

Q&A

Can I tell my manager about a potential acquisition target Secureworks is considering?

It depends. To protect the confidentiality of Secureworks' strategic business plans and ensure we can comply with all applicable legal requirements, Secureworks places tight controls around our acquisition projects. Only certain essential team members are informed of a potential acquisition and they are subject to strict nondisclosure obligations. So, unless you know your manager is already part of the team working on that project, you should check with the project manager before talking to your manager about it.

Responsible travel and entertainment

What we believe

Responsible business travel and entertainment enhances our profitability and reputation. Team members are expected to truthfully, accurately and completely record travel and entertainment expenses.

What it means for you

Use Secureworks funds only for legitimate business purposes and don't spend more than necessary. Follow company policies regarding the use of corporate credit cards, preferred travel vendors, necessary management approvals, receipts, expense reports and other travel-related matters.

Be honest and accurate when submitting expense claims for reimbursement, and never use Secureworks funds for personal travel or entertainment, or to supplement your income.

Don't go to places that would reflect negatively on Secureworks, such as a sexually-oriented business. Expenses incurred at these establishments will not be reimbursed. These venues are not acceptable for business entertainment even if expenses are not submitted for reimbursement.

Did you know . . .

Expense report fraud includes submitting fictitious receipts, reporting inaccurate mileage, falsifying client names and fabricating business purposes.

Speaking on Secureworks' behalf

What we believe

Secureworks' public statements must be carefully managed to ensure accuracy, fairness and compliance with legal requirements, as well as to protect our reputation and ensure consistency with our mission, values and brand.

What it means for you

Secureworks uses certain distribution channels—such as press releases, media and analyst conferences and statements on our company website—to communicate our company's official position to the public. Use of these channels is limited to authorized individuals and information shared must be valid, accurate and approved for public release.

The Secureworks External Communications Policy allows only authorized team members to provide company information and communicate on behalf of the company to media, analysts, investors and other public forums. This applies to digital communications, including social media, as well as to traditional forms of communication.

Refer all inquiries from Reporters, invitations to participate in External Surveys and Benchmark Studies, and requests to provide Expert Witness Testimony to the Secureworks Media Relations team. Clear all Blog postings and Letters to the Editor copy to the Secureworks Media Relations team. Refer all inquiries from Industry Analysts to the Secureworks Analyst Relations team. Refer all inquires from Investor Analysts and Investors to the Secureworks Investor Relations team. Contact information for Media Relations, Analyst Relations and Investor Relations teams is available in the External Communications Policy.

Contact Events Marketing if you are invited to speak publicly at conferences, seminars, trade shows or other events - before accepting the invitation.

Contact the Legal Department if you receive an inquiry from government personnel about public policy, regulatory or enforcement matters.

Q&A

A local newspaper reporter contacted me about Secureworks' plans for expansion in the area. How should I respond?

Obtain the person's name, email address, phone number, publication or other affiliation, and deadline. Tell the person that a Secureworks spokesperson will call them back. Provide the caller information to the Secureworks Media Relations team.

Contracting authority

What we believe

We enter into contractual relationships with clients, business partners and other stakeholders objectively and in the best interests of Secureworks.

What it means for you

To promote efficiency, ensure compliance with legal, accounting and financial reporting requirements, and protect Secureworks' assets from fraud, waste and abuse, Secureworks has established policies, procedures and controls governing the negotiation and approval of contracts between Secureworks and its clients, suppliers, business partners and other stakeholders.

Authority to enter into and sign contracts on Secureworks' behalf has been delegated to different Secureworks team members depending on the nature, parties, scope and financial value of the contract involved.

If you are involved in negotiating any contracts for Secureworks, make sure you understand and follow Secureworks' contracting policies, act only within the authority delegated to you under those policies and related signature authority matrices, and ensure that all necessary approvals from the Finance, Accounting, Global Procurement, Contracts Management and Legal Departments have been obtained.

Q&A

A channel partner placed an order. The order has been approved and downloaded and is in process. The partner just contacted me and said he is concerned his customer might not be able to pay. I don't want to cancel the order so I told him I would help him find other buyers if that happens. Is this OK?

No, not unless you negotiate a formal amendment to the original order and obtain all the necessary approvals from Legal, Finance and Accounting. If you fail to take these steps, your oral agreement is an impermissible "side letter" or "unauthorized commitment" and it changes the terms of the original order which could affect when Secureworks is able to recognize the revenue from the sale.

Our commitment to our clients

Our clients are the reason we exist and they rely on us to listen and provide security solutions that will help protect them. To earn and maintain their trust, we are committed to doing business fairly, honestly, legally and ethically wherever we operate in the world.

Keeping our promises to our clients

What we believe

We build long-term client relationships by providing quality solutions and services at reasonable prices and by demonstrating honesty and integrity in all our interactions. We comply with all laws prohibiting deceptive trade practices.

What it means for you

Everything we tell clients and prospects about our solutions and services—in our advertising, sales and marketing communications or otherwise—must be truthful, accurate, complete and understandable.

Don't mislead clients by exaggeration, by omitting vital information or by advertising solutions, features or services you are not confident we can deliver.

Make sure you comply with all internal requirements relating to the review and approval of advertising and marketing communication materials. Seek guidance from the Legal Department when you are unsure or have questions.

Did you know . . .

> Regarding advertising materials, a good rule of thumb is this: information should be disclosed in the body of the advertisement if it would be key to the client's decision to purchase from us.

Protecting the privacy of client personal information

What we believe

We earn the trust of our clients and others by keeping personal information safe and complying with the privacy and data protection laws of the countries in which we do business.

What it means for you

Numerous laws in each country regulate the collection, use, storage, disclosure, and deletion of personal information. Personal information can include general information such as name, home address, email and IP address, company name and telephone numbers. It also includes more sensitive personal information—such as financial records, government-issued identification numbers like Social Security numbers, credit scores, credit card numbers, medical records, educational or employment records , sexual orientation, race, family status and political or religious affiliations—which may be subject to additional specialized legal or contractual obligations.

We take our obligations regarding protection of personal information very seriously. When accessing or handling personal information—regardless of who it belongs to, how it was obtained or where it is stored—team members must comply with applicable laws and regulations, as well as Secureworks policies, contractual obligations and voluntarily-adopted standards. Keep it safe, secure and do not lose it. Failure to meet these standards may result in disciplinary action up to and including termination.

Make sure you use only responsible and lawful means if you collect personal information about clients or prospects on behalf of Secureworks, and be sure any personal information collected is only for legitimate business-related purposes. Safeguard personal information carefully and do not disclose it to others or use it for marketing or other purposes except when you know doing so is compliance with advance notice, authorization, consent and other requirements. Always respect clients' and prospects' communication preferences. Your local contacts in the Legal Department and CISO team can advise you on what is needed for specific situations.

When providing support or other services to our clients, access personal information or other private data only to the extent necessary to carry out the required service. Do not collect information that you do not need.

Safeguard client payment and other financial information carefully, and never use or disclose it inappropriately.

Select business partners for marketing or other services who share our commitment to protecting and appropriately using personal information.

When providing services—including managed security, consulting, compliance, incident response, intelligence and other services - to our clients, always respect the privacy of their customers, employees and other constituents including patients and students. Comply with any special legal or contractual requirements regarding these constituents' personal information and other sensitive information. Team members working on a client site or directly with a client's information technology resources must also comply with the policies and standards of both Secureworks and the client for protection of personal information.

If you suspect that personal information has been used or disclosed inappropriately or that a data security breach has occurred, immediately contact the Legal Department and the CISO Team. They will take appropriate action and manage compliance with applicable notification or other obligations relating to relating to data security incidents or unauthorized disclosures of personal information.

For additional information, review the Information Security Policies and Control Standards by clicking the Corporate Security Office link on our Intranet, and consult our Privacy Policy.

Did you know . . .

Protecting personal information is everyone's responsibility at Secureworks. The company has Information Security Policies and Control Standards which must be adhered to. Review these policies and controls by clicking the Corporate Security Office link on our Intranet, and consult our Privacy Policy.

Compliance with government contracting requirements

What we believe

Secureworks provides intelligence-driven security solutions to clients that help protect businesses and citizens around the world. We are proud to serve these clients and comply with all laws, regulations and contractual requirements relating to government procurement.

What it means for you

While we must behave legally and ethically in connection with every client relationship, contracts with government clients, or commercial transactions that are financed in whole or in part by government agencies or with public funds, have additional requirements and obligations.

Always follow the rules

If you are involved with these kinds of clients or transactions—whether in connection with bids or tenders, negotiation, administration or fulfillment—be sure you understand and comply with all applicable statutory, regulatory and contractual provisions and controls. This includes complying with security clearance requirements and obligations to protect classified or confidential information. If you have questions about any requirements associated with government-related contracts, seek guidance from the Legal Department.

Likewise, be diligent in requiring that channel and other business partners providing goods or services in connection with government or publicly-funded contracts meet all qualification and performance standards and requirements.

Secure business the right way

Information submitted in connection with bids or tenders for government contracts must be current, accurate and complete.

Never offer bribes, kickbacks or preferential treatment in connection with a government contract. With limited exceptions, you are also prohibited from providing anything of monetary value to government employees or their family members. This includes gifts, entertainment, travel, lodging, services, discounts and meals.

Ethical fulfillment

All reports, certifications, statements and other information submitted in connection with a government contract should be timely, accurate and complete.

Never make unauthorized or incorrect charges, or submit inaccurate information regarding costs or pricing in connection with government contracts. Likewise, do not make substitutions or deviations from contract requirements and specifications without obtaining required approvals from Secureworks and the applicable government official.

Report issues and concerns

If you suspect any illegal or unethical conduct on the part of any Secureworks team member or business partner in connection with a government contract, report the matter immediately using any of the available internal reporting avenues. The appropriate Secureworks team members will independently investigate the issue and comply with applicable legal and contractual self-reporting requirements. You may also contact the relevant government authority with your concern.

Did you know . . .

Secureworks' internal reporting procedures are available to business partners and other non-employees. Non-employees are encouraged to report potential violations involving Secureworks in connection with a government contract.

Our commitment to our business partners* and communities

We believe that being a responsible corporate citizen is central to our mission and values, allowing us to inspire trust among our business partners and motivate team members to give back to our communities.

*"Business Partners" is a generic reference to vendors, suppliers, agents and other non-client third parties with whom Secureworks does business. Use of the term "partner" does not imply the existence of a legal partnership relationship or the creation of partnership rights.

Anti-bribery and anti-corruption

What we believe

We are committed to winning business only on the merits and integrity of our solutions, services and people. Corruption impedes the development of trustworthy markets; it hurts our company and the communities where we do business. We do not tolerate bribery or corruption, regardless of where we are located or where we do business.

What it means for you

Never provide anything of value that could be perceived as a payment in order to obtain or retain business with Secureworks, direct business to Secureworks or others, or otherwise obtain an improper business advantage with a government official.

Always comply fully with the anti-bribery and anti-corruption laws of the countries in which we do business, including the Foreign Corrupt Practices Act (FCPA)) and the UK Bribery Act of 2010. The FCPA applies to the actions of our company, our team members and third parties who work on our behalf anywhere in the world.

Regardless of local practices or competitive intensity, you must avoid even the appearance of bribery when dealing with any individual, including government officials, employees of state-owned or controlled enterprises, and officials of international organizations and or political parties, and employees of state-owned or controlled enterprises government officials, as well as officials of international organizations and political parties.

For additional information, please consult the applicable Secureworks policies and standards.

Did you know . . .

Complex rules govern the giving of gifts, entertainment and other business courtesies to government officials. What may be permissible for commercial clients may be illegal when dealing with the government. If you have questions about these rules or how the rules apply, seek guidance from the Legal Department or CISO Team.

Political contributions and activities

What we believe

We believe in advocating for public policies that help maximize the benefits that information technology can bring to people everywhere.

What it means for you

Team members are encouraged to be responsible citizens who participate in civic and political activities, provided their activities are lawful and appropriate, and are conducted on their own time and at their own expense.

Do not use Secureworks funds or assets, including facilities, equipment or trademarks in connection with your personal political activities or interests. Use care not to give the impression that Secureworks supports or endorses any candidate, campaign or issue with which you are personally involved.

See the Code provisions on Avoiding conflicts of interest and Using information technology and other resources for additional guidance.

Follow all laws as they relate to the ability of corporations to make political contributions or engage in lobbying or other political campaign activities.

The Government Affairs team is responsible for coordinating Secureworks' activities with government officials and policy makers in compliance with applicable laws. Team members must not communicate with public officials regarding Secureworks-related policy matters or claim to represent Secureworks with policy makers except as authorized or directed by the Government Affairs team.

Q&A

I have a good friend who is running for political office and has asked if I would endorse him at a rally being held outside of business hours. Is that a problem?

No. Just be sure to make it clear that your endorsement is your own personal action and that you are not speaking on behalf of Secureworks.

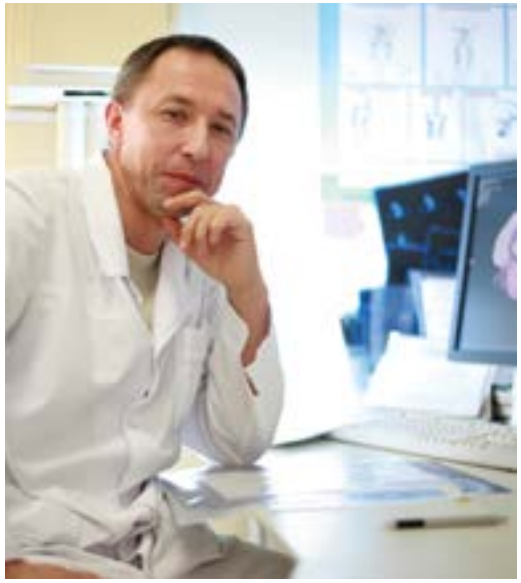
Fair competition

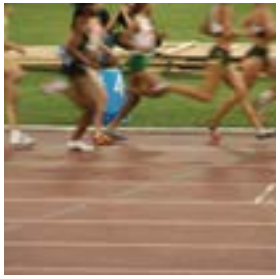
What we believe

We will win in a fair and competitive marketplace by providing clients with security solutions and services at reasonable prices. We abide by laws designed to preserve free and open competition.

What it means for you

The U.S. and other countries have adopted laws prohibiting or regulating transactions and relationships that could have the purpose or effect of limiting competition. These laws apply to business practices of dominant companies, agreements and dealings between competitors and others that limit competition, and mergers and acquisitions. All team members must compete fairly and vigorously in compliance with applicable competition-related legal requirements, agreements with regulators and Secureworks policies and procedures.





Agreements to avoid

Competition laws are complex so you should always consult with the Legal Department before entering into any discussions with competitors, clients, channel or other business partners about agreements or arrangements—express or implied—that could have the effect of limiting competition. This includes arrangements that would limit Secureworks' or others' ability to:

- sell or resell certain solutions or services;
- set their own prices or terms and conditions of sale or resale;
- sell or resell in certain territories or markets;
- bid for or do business with certain clients or business partners or suppliers; or
- hire employees or set employee compensation.

Be especially careful when interacting with competitors in connection with benchmarking, industry associations, standards-setting bodies or while attending seminars or conventions. To avoid even the appearance of an agreement, you should never discuss with competitors such things as prices, terms of sale, territories, clients, bids, product lines, service offerings, volumes, costs, profits, market share, salaries, hiring practices, distribution methods or relationships with suppliers.

Did you know . . .

Competition laws may also be referred to as "antitrust," "monopoly," "cartel" and "price fixing" laws. All are designed to preserve fair and open competition.

Don't jump the gun

Comply with legal requirements relating to mergers, acquisitions and joint ventures. Always follow guidance from the Legal Department when evaluating prospects, and don't begin exercising control or integrating a target company until all necessary government approvals have been obtained.

Do unto others

Gather information about our competitors only from public sources and through client feedback. Don't gather or use confidential information belonging to competitors—especially if you know it was obtained inappropriately or is subject to others' confidentiality obligations. Refrain from unjustifiably disparaging or criticizing competitors' products or services.

Q&A

I was recently at a trade association meeting and overheard one of our competitors talking about their pricing strategy. I immediately left the room. Was that the right thing to do?

Yes. Removing yourself from the meeting reduces the risk that someone might think you were trying to fix prices or engage in other inappropriate activity. Contact the Legal Department to report the incident and do not share any information you may have heard at the meeting.

Respecting the intellectual property of others

What we believe

Intellectual property such as trade secrets, patents, unique ideas and inventions, creative works and trademarks, are valuable information assets. We protect our intellectual property and respect the intellectual property of others.

What it means for you

Do not copy, share or modify third-party copyrighted materials unless you or Secureworks has first obtained written permission from the copyright holder. Improper use—whether for business, personal or Secureworks internal use—of copyrighted material can subject you and Secureworks to possible civil and criminal penalties and other serious consequences.

Secureworks uses third-party hardware systems and software programs under licensing agreements that may restrict their use and duplication. Comply with applicable license restrictions and Secureworks policies relating to the use and duplication of these systems and programs.

Do not infringe on patents or other intellectual property belonging to others. Use care when developing products or processes for Secureworks and take steps to ensure that the ideas and innovations you develop are truly your own.

Do not infringe on other companies' trademarks or trade names. Always consult with the Legal Department when naming product or service offerings.

If you are contacted by someone who wants to sell or license to Secureworks an idea, patent, domain name, design, process, methodology, or other creation or invention, immediately contact the Legal Department and do not enter into any agreements or substantive discussions.

Comply with Secureworks' obligations under non-disclosure agreements entered into with clients and business partners.

Honor confidentiality obligations you may have to third parties such as former employers, and don't encourage others to engage in illegal or unauthorized sharing of third-party confidential information they may have.

For additional information, please consult the applicable Secureworks policies and standards.

Q&A

Our new team member has a lot of industry experience that we would like to use to our advantage. Is it OK for him to share with us what he knows?

Yes and no. It's OK and even helpful to learn from a new team member, but be careful. The team member can share his general knowledge and experience, but he can't share confidential information, trade secrets or other intellectual property belonging to his former employer.

I attended a skills-building workshop conducted by an outside provider. The materials were great. Can I make copies of them for my team members or adapt them for a workshop I will lead here at Secureworks?

No, not unless the outside workshop provider explicitly grants permission. Unauthorized reproduction, distribution or adaptation of copyrighted materials is infringement, even if only used for internal purposes.

Preventing money laundering and terrorist financing

What we believe

We abide by all laws designed to deter criminal enterprise, keep us safe from terrorism and protect the national security of the countries where we do business.

What it means for you

Money laundering is the process by which funds generated from criminal activity such as drug trafficking are moved through legitimate businesses in order to hide their criminal origin. Terrorist financing refers to funding for terrorist activities and can come from legitimate or criminal sources.

Team members must never knowingly facilitate either money laundering or terrorist financing, and must take steps to prevent inadvertent use of Secureworks' business activities for these purposes.

Be vigilant and exercise good judgment when dealing with clients or business partners. Know who they are, what kind of business they are in, and where their funds come from.

Immediately report any unusual or suspicious activities or transactions such as attempted payment in cash or from an unusual financing source, arrangements that involve the transfer of funds to or from countries or entities not related to the transaction or customer, unusually complex deals that don't reflect a real business purpose, or attempts to evade record-keeping or reporting requirements.

Did you know . . .

Both money laundering and terrorist financing are illegal in the U.S. and most other countries.

Charitable contributions and activities

What we believe

Secureworks is committed to giving back to the communities where our team members live and work. We make charitable contributions consistent with our giving goals and encourage team members to support their communities through appropriate volunteer activities.

What it means for you

Many Secureworks team members volunteer their time, talents and energy to support charitable causes and non-profit organizations. Secureworks is proud of our team members' generous spirit and encourages these kinds of activities provided they do not conflict with SecureWorks' interests or reflect negatively on Secureworks.

Volunteer efforts in support of Secureworks-sponsored community involvement programs may be done during work hours if approved by your manager in advance. All other volunteer efforts must be done on your own time and must not jeopardize your productivity or ability to perform your duties for Secureworks.

Occasional and limited use of Secureworks equipment and resources for personal charitable activities is permissible, but more than minimal use would need to satisfy the requirements for charitable contributions from Secureworks.

SecureWorks makes contributions only to certain qualified non-profit organizations. As a Secureworks team member, you may receive requests for charitable contributions from Secureworks. Whether the request involves donations of money, new or used computer equipment, services, software, event sponsorship or anything else of value, all charitable contributions must be in compliance with applicable laws, Secureworks' and/or Dell's Corporate Charitable Contribution Policy.

See the Code provisions on Avoiding conflicts of interest and Using information technology and other resources for additional guidance.

Did you know . . .

U.S. law requires organizations to ensure that their charitable donations do not aid terrorists or organizations that support terrorism.

Compliance with trade laws

What we believe

We serve clients and engage with business partners all over the world. By abiding by trade laws, we enable commerce and help secure organizations in all the countries where we do business.

What it means for you

Secureworks operates all over the world and we comply with applicable country laws regarding import or export of services, software and technology.

Since Secureworks is a U.S.-based company, we must comply with U.S. trade regulations in every international transaction. We cannot export solutions or services to countries that are embargoed by the U.S. government, sell to certain persons and entities or for specific end-uses, or release certain kinds of technology or software.

Consult with the Legal Department and CISO Team before making any commitment to export solutions, services, software or technology from the U.S. or another country, or if you have questions about Secureworks' or your compliance obligations in this area.

Always truthfully, accurately and completely report information regarding any imported solutions or services. Many countries have customs laws requiring that we determine the correct classification, value and country of origin for all our imports. We must be able to demonstrate by a documented, auditable trail that we have exercised reasonable care to ensure our imports have complied with all applicable laws and regulations.

For more information, refer to Secureworks' Global Trade Compliance Policy

A final word

Thank you for reading Secureworks' Code of Conduct, "How We Win." We hope you find it useful in guiding your behavior and decisions as you carry out your daily activities at Secureworks. Our Intranet site will always reflect the current version of the Code with the latest revisions and updates, as well as a link to the Corporate Security Office portal which contains relevant compliance and ethics policies, and control standards.

Please tell us what you think. We welcome your input on any aspect of our Code of Conduct or our ethics and compliance-related policies and procedures.

Please send your feedback to AskHR@SecureWorks.com.

Secureworks Ethics and Compliance

Contacts

Ethics

Compliance

Legal Department

CISO Team

Procurement

Human Resources

Resources

Secureworks EthicsPoint Helpline

Secureworks Legal Portal

Corporate Security Office Portal

Human Resources Portal

Global Gifts & Entertainment Policy