CODE OF CONDUCT

(U.S. Employees)

March 2024

TABLE OF CONTENTS

1 INTRODUCTION - OUR CODE AND AT-WILL EMPLOYMENT

You are essential to the work performed at Acrisure, LLC and its affiliates (collectively, "Acrisure" or the "Company"). We want you to understand how we do business. This Code of Conduct (the "Code"), therefore, explains key expectations we have for you and what you can expect from us. It supersedes and replaces all inconsistent policies, practices, and guidelines.

The Code is written to protect your rights and Acrisure's rights. It is a statement of policies and not intended to be a contract guaranteeing any specific terms of employment, nor is it intended to otherwise create any other contractual obligations with respect to your employment. You are employed "at will"; any contrary statements are not binding upon Acrisure, unless in writing and signed by an Acrisure Officer. Nothing in this Code can be construed to contradict, limit or otherwise affect your right or Acrisure's right to end your employment relationship at any time with or without notice or cause. Acrisure reserves the right to interpret and administer the provisions of this Code as needed. Except for the policy of at-will employment, which can only be changed in writing by an Acrisure Officer, Acrisure has the maximum discretion permitted by law to change, modify, add, suspend, interpret or discontinue any element of this Code, with or without cause or notice at any time. However, oral statements or representations cannot supplement, change or modify the provisions in this Code. Any change to this Code will be communicated through an update that gets posted on the HR page of our latest platform for employee engagement.

If any provision of this Code is found to be unenforceable or void for any reason, such invalidation will not affect any remaining provisions, which will remain in force. This Code is not intended to preclude or dissuade employees from engaging in legally protected activities, nor intended to restrict communications or actions protected or required by state or federal law.

In accordance with the laws of the particular state or city where you are employed, there may also be an Addendum, located at the back of this Code. Any such Addendum supplements the provisions contained in this Code for those employed in the state or city identified in the Addendum. Where this Code and an Addendum to this Code conflict, the Addendum states Acrisure's policy with respect to its employees in the state or city identified in the Addendum.

We ask that you review and familiarize yourself with the contents of this Code, keeping it handy as a reference source. ***Once you review this Code, please sign the required acknowledgement in the form provided.***

2 PROFESSIONALISM AND EQUAL EMPLOYMENT OPPORTUNITY

2.1 BUSINESS PRACTICES, EMPLOYEE CONDUCT, AND ETHICS – OVERVIEW

The successful business operation and reputation of Acrisure is built on the principles of fair dealing and your ethical conduct. Our reputation for integrity and excellence requires careful observance of the spirit and letter of all applicable laws and regulations, as well as an unwavering commitment to the highest standards of conduct and personal integrity. As an Acrisure employee, you owe a duty to Acrisure and its clients to act in a manner that will warrant the continued trust and confidence in Acrisure.
Acrisure is firmly committed to complying with its legal and ethical obligations under all local, state, and federal laws. As a result, we expect you to comply strictly with all legal and ethical obligations. Our philosophy can be implemented only if you recognize your responsibility to treat everyone in an ethical manner. The policies in this Code provide details on these commitments and expectations. Your failure to fulfill your responsibilities under any of these policies may result in disciplinary action, up to and including separation from employment.

2.1.1 Responsibility and Methods to Report Concerns

You are responsible for carrying out and monitoring compliance with our Code. If you are subjected to, observe or otherwise become aware of any conduct that you believe violates any applicable law or this Code, you must promptly speak to, write, or otherwise contact your Leader, your Leader's supervisor, Human Resources or the Company's Ethics Hotline so that it can be investigated right away. Acrisure emphasizes that you are not required to raise concerns first to your Leader if your Leader is the individual who engaged in the conduct that concerns you.

If you have not received a satisfactory response within five (5) business days after reporting any conduct that you believe violates any applicable law or this Code, please immediately contact Human Resources.

Although not mandatory, it would be best to communicate your concerns in writing. It should be as detailed as possible, including the names of all individuals involved and any witnesses. Acrisure will take all necessary steps to investigate any potential violations of any applicable law and/or our policies and will take appropriate action to correct any violations or incorrect perceptions that may exist.

Additionally, any Leader or other supervisor who observes, receives a report, or otherwise becomes aware of potential Code violations must immediately report such conduct to Human Resources or via the Company's Ethics Hotline so Acrisure can take prompt action.

If you believe another employee has been subjected to Code violations, you *must report the matter as described above*, even if the employee reporting the incident asks that the incident be kept confidential or that no action be taken.

Where the matter is more serious, you feel your concern has not been addressed, or you prefer not to raise it with your Leader or the Human Resources Department for another reason, you should contact one of the following:

- your relevant Whistleblowing Contact; or
- the Legal Department.

You should consult Acrisure's Global Whistleblowing Policy, which can be found Here, for further information regarding reporting concerns.

2.1.2 Investigation and Remediation

When Acrisure receives a complaint of conduct that violates this Code or other Company policy, we will timely conduct a fair, impartial, and thorough investigation by qualified personnel. The investigation will provide all parties appropriate notice and an opportunity to respond. Acrisure will maintain confidentiality to the extent it is possible and practicable to do so under the circumstances; however, Acrisure cannot promise complete confidentiality, as its commitment to investigate and take corrective action may require disclosure of information to individuals with a need to know. Depending on the circumstances, Acrisure's investigation may include private interviews with the person who filed the complaint, with witnesses to the alleged conduct-at-issue, and with the person(s) whose alleged conduct is the subject of the complaint. The investigation will be documented and tracked for reasonable progress.

When we have completed our investigation, we will consider appropriate options for remedial actions and resolutions, if warranted under the circumstances. Acrisure will impose appropriate disciplinary action, up to and including separation from employment. Acrisure will impose appropriate discipline, up to and including separation of employment, to any supervisor or manager who knows about conduct in violation of this policy and took no action to stop it or failed to report the conduct.

2.1.3 Anti-Retaliation

Acrisure strictly prohibits and does not tolerate unlawful retaliation against any applicant, employee or intern for good faith reports of conduct that violates this Code, or cooperating in related investigations. All forms of unlawful retaliation are prohibited, including any form of discipline, reprisal, intimidation, or other form of retaliation for participating in any activity protected by law.

Examples of protected activities include, but are not limited to:

- Submitting a good faith internal complaint (written or oral) with Human Resources or management specifically opposing unlawful discrimination or harassment or complaining about violations of wage and hour law (for example, if you believe you have been sexually harassed or not paid overtime you are owed).
- Filing a good faith complaint of unlawful discrimination or harassment with the US Equal Employment Opportunity Commission (EEOC), a state or local fair employment practices agency (FEPA), or in court.
- Participating in Acrisure's internal investigation into allegations of discrimination or harassment.
- Supporting another employee's internal or administrative complaint of unlawful discrimination (by, for example, testifying or providing an affidavit in support of a coworker who has filed a discrimination complaint with the EEOC or state or local FEPA).
- Filing a good faith complaint with the US Department of Labor (DOL), state or local wage and hour agency, or in court about wage and hour violations or unfair pay practices, or participating in a wage and hour investigation or audit conducted by the DOL or state/local administrative agency.
- Requesting an accommodation under the Americans with Disabilities Act or state or local anti-discrimination statutes.

- Requesting or taking leave under the Family and Medical Leave Act or pursuant to an applicable state leave statute.
- Filing a workers' compensation claim.

The examples above are illustrative only, and not exhaustive. All forms of unlawful retaliation for any protected activity are prohibited. For further discussion of the Company's anti-retaliation policy, please see the Company's Global Whistleblowing Policy, which can be found Here.

2.2 EQUAL EMPLOYMENT OPPORTUNITY, NON-DISCRIMINATION, AND ANTI-HARASSMENT

Acrisure is an equal opportunity employer committed to compliance with all applicable federal, state and local fair employment practice laws providing equal employment opportunities and prohibiting discrimination and harassment in the workplace. We are all responsible for fostering a respectful, inclusive and productive work environment that is free from discrimination and harassment. You are expected to comply with and Acrisure will strictly enforce its Equal Employment Opportunity, Non-Discrimination, and Anti-Harassment policies, which can be found in Acrisure's Experience Policies.

2.3 CONFLICTS OF INTEREST

This policy sets forth guidelines relating to situations that could involve a conflict between your personal interests and those of Acrisure. Generally, you must avoid situations where your personal interests, including other business interests, conflict with Acrisure's interests – or when it could reasonably be perceived as being in conflict.

While employed by Acrisure, you are expected to devote your full energies and efforts to your job with the Company. You can work for other employers where such work does not interfere with your obligations to the Company. The following types of outside employment are strictly prohibited:

- Other employment that casts doubt on your ability to objectively act in Acrisure's best interest or is otherwise incompatible with your position with Acrisure;
- Other employment that impairs or has a detrimental effect on your work performance with Acrisure.

A conflict of interest also may exist where you:

(1) approve payments to;
(2) report to or report to a person who is directly managed by; or
(3) exercise authority with respect to hiring, promotional or compensation related decisions for a relative, spouse or other persons with whom you have a romantic relationship.

If you have any influence on transactions involving purchases, contracts, or leases it is imperative that you disclose this information, the existence of any actual or potential conflicts of interest, to an Officer of Acrisure as soon as possible so that safeguards can be established to protect all parties.

You have an ongoing responsibility to disclose any situation that creates, may create, or has the appearance of creating a conflict of interest.

2.4 ADDITIONAL CORE PROFESSIONALISM EXPECTATIONS

Acrisure expects you to conduct yourself in a professional, respectful, ethical and legal manner while at work. To supplement the preceding policies regarding our standards of conduct and provide guidance concerning unacceptable behavior, the following is a non-exhaustive list of conduct that should not take place in the work environment and will be addressed through the processes outlined:

- Any violation of Acrisure policy, including any policy in this Code and in Acrisure's Experience Policies.
- Misappropriation or unauthorized use of money, credit, property, or equipment of the Company or belonging to another employee, a client, a supplier, or a visitor.
- Dishonesty of any kind, including fraud, asking another employee to lie, withholding the truth, or falsifying time sheets or any Company documents or files.
- Rude, abusive, or threatening language or outbursts of anger toward management, employees, clients, or others.
- Engaging in any action on or off Company premises that reflects unfavorably on the organization and its reputation, including criminal or illegal behavior of any kind.
- Possessing, disclosing, misusing or failing to maintain confidential information or trade secrets or engaging in direct competition with the Company while employed by the Company.
- Unsatisfactory job performance, including, but not limited to, failure to perform assigned duties or failure to treat a client in a professional, courteous manner, etc.
- Participating in an unsafe work practice, failing to observe safety rules or procedures, or disregarding any established safety rule.
- Solicitation of any type (except charitable donations approved by Acrisure), or selling or passing out any products, information or documents on Company property or during work time. (Work time means those hours that you are on duty, excluding breaks, meal times, and other specifically designated periods during the day when you are not engaged in performing work duties.) Nothing in this policy is intended to restrict your rights under the National Labor Relations Act.
- Directly, or indirectly, for yourself or any other person, corporation, firm or entity, redirecting or encouraging the redirection of business or employees away from the Company. This obligation continues for a period of two years after your employment relationship with the Company terminates.

3 PROTECTING ACRISURE INFORMATION AND SYSTEMS

3.1 DEFINING SENSITIVE DATA

Sensitive and non-public personal data (hereinafter "Sensitive Data") includes, but is not limited to, Protected Health Information (PHI), social security numbers (SSN), bank account information, cardholder data (personal account numbers, PINs, card verification codes, and expiration dates), passwords, encrypted data, personally-identifiable information (names, addresses, customer numbers), and Acrisure confidential materials, including, but not limited to, employee information, acquisition strategies, rating techniques, pricing plans, rates, coverage, business plans, strategies, trade secrets, vendor lists, client lists

and any materials reflecting clients' preferences and buying history, employee information, network infrastructure, or financial information.

3.2 ACCEPTABLE USE

Acrisure is committed to safeguarding the confidentiality and privacy of Sensitive Data belonging to Acrisure, its customers, employees, and vendors, and all other parties doing business with Acrisure. We have implemented the following policies related to information security, which, along with any other information security-related policies subsequently issued by Acrisure, shall apply to you (and can be found Here):

- Acceptable Use Policy;
- Bring Your Own Device Policy ("BYOD Policy");
- Security Awareness and Training Policy;
- Password Creation and Management Policy;
- Mobile Device Policy;
- Security Policy Exception; and
- Email and Internet Use Policy

3.3 ACCEPTABLE USE POLICY

Acrisure's Acceptable Use Policy is intended to safeguard IT Assets from misuse and unauthorized access, as well as to ensure compliance with applicable laws, regulations and industry standards and best practices. You are responsible for exercising good judgment regarding the appropriate use of IT Assets. Acrisure's information systems and networks (collectively, "IT Assets") include email, Internet browsers, word processing software, telephone systems, and all other computer hardware and software. Acrisure's information systems and networks are the sole property of Acrisure and are to be used for Acrisure business-related tasks in accordance with this Policy. This Policy also applies to all equipment, buildings, and other Acrisure assets owned, leased, or operated by Acrisure. This Policy also applies to all authorized Bring Your Own Device ("BYOD") devices to the extent they are used to access and/or transmit Acrisure content or otherwise conduct Acrisure business.

All uses of IT Assets, including the creation and storage of work product, Internet access, social media messages and posts, and all other forms of electronic and other written communication, are subject to monitoring and recording by Acrisure at any time. Please be aware that you have no expectation of privacy in any use of Acrisure's information systems and/or networks.

3.3.1 Asset Ownership and Management

- Acrisure does not intend to unreasonably intrude; however, we reserve the right to monitor the usage of Acrisure systems at any time without notifying you. We also reserve the right to withdraw Acrisure system access at any time without prior notice. All data created on Acrisure systems remains the property of Acrisure.
- Personal devices can be used for Acrisure business as outlined in the Acrisure BYOD Policy. Upon your request, you will provide their BYOD device to your manager and/or a member of the Information Security team so that they can verify that all security policies are being followed. By

participating in BYOD, you are authorizing Acrisure to delete Acrisure-related data from the BYOD device at any time.

- No Acrisure network, mobile device, computing asset or other IT resource may be used at any time for an unlawful or prohibited purpose. For example, you may not browse, download, or upload content from pornographic, gambling, hate-related sites or any sites deemed to be malicious.
- For security, compliance, and maintenance purposes, Acrisure authorized personnel will monitor and audit equipment, systems, and network traffic. Any software, device or any mechanism that would interfere, disrupt, or evade such monitoring and audit activity is prohibited. Devices that interfere with other devices or Users on the Acrisure network are not permitted. No technology will be deployed that will block or disable Acrisure Information Security tools and technology.
- All Acrisure assets, including, but not limited to, BYOD devices that are utilized for work activity are subject to Acrisure legal obligations including legal hold, forensic analysis, subpoena, search warrants, and national security letters. You may be required to surrender their asset or device to fulfill these lawful requirements.
- Acrisure periodically audits its networks and systems to ensure compliance with this Policy, including the use of content filtering.

3.3.2 Your Responsibilities

- You are responsible for exercising good judgment regarding the appropriate use of Acrisure's assets and BYOD devices.
- You should read, understand, and agree to comply with this Policy upon hire and periodically thereafter.
- You should be personally aware of your daily responsibility in protecting Sensitive Data.
- You should consult with your manager or the Acrisure Chief Information Security Officer ("CISO") about any confusion around your roles and responsibilities and how to apply this Policy.
- You should let your manager know if your job responsibilities require less or more system or building access.
- You should contact Acrisure IT if "locked out" of a system.
- You agree that any mobile device connected to the Acrisure network will be managed by the Acrisure Mobile Device Management System ("MDM") or Mobile Access Management ("MAM"). Any Acrisure or BYOD that connects to the Acrisure network will be subject to the restrictions of the MDM or MAM software.
- You should notify Acrisure IT within 24 hours, or, if possible, sooner, if a laptop or mobile device is lost or stolen. Acrisure IT will be responsible for utilizing department procedures and the Acrisure Incident Response Plan to triage and mitigate any potential risk.
- You should understand that the data created on Acrisure systems remains the property of Acrisure. Management cannot guarantee the privacy of personal data stored on any server, system, storage, or device maintained or owned by Acrisure, and you do not have an expectation of privacy for any personal data created or stored on Acrisure systems.
- You are responsible for exercising good judgment regarding personal use of Acrisure workstations, equipment, or devices. Personal use for personal profit is not allowed on Acrisure workstations, equipment, or devices. If there is any uncertainty about personal use, consult your manager.
- You should understand that laptops and other portable devices will:

    - Be taken home at the end of the shift or be locked and not visible if the device remains onsite
    - Not be left visible in unattended vehicles, as this presents a risk of both theft and damage.
- You should lock your workstation when you walk away from your desk.
- You should understand that removable media, such as external hard drives, USB sticks, and SD cards, should be used with caution. Please follow these guidelines:
    - Do not use any media distributed from a source other than Acrisure IT without approval from the Acrisure IT. The use of non-approved removable media is strictly prohibited.
    - Media found in drawers, on the floor, or anywhere around the building should be turned in to Acrisure IT to be checked for malicious payloads and identification of ownership.
    - Media provided to Acrisure by a vendor, such as at a trade show, or by a customer must be scanned by Acrisure IT before using in an Acrisure computer
    - Do not use any removable media containing Acrisure information or business in any non-Acrisure owned and operated systems.
- You understand that the CISO will determine what, if any, personally owned devices will be allowed onto the corporate network and will publish a list of acceptable devices and/or device types. Any BYOD device allowed to access the Acrisure network must comply with the BYOD Policy.
- You agree that all systems and devices, regardless of ownership, that are connected to Acrisure networks will be continually executing approved virus-scanning software per the Acrisure Written Information Security Plan.

3.3.3 Leader Responsibilities

- Once a leader determines that an individual no longer requires the use of a system or access to a building or area, s/he should open an Acrisure IT ticket requesting removal of access.
- Leaders should engage the CISO to ensure that contracts with third parties that could/will have access to Sensitive Data include appropriate security language.

3.3.4 Unacceptable Use

The activities outlined in this section are prohibited. Users may be exempted by the CISO from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services). Under no circumstances are you authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Acrisure-owned resources or Acrisure systems. The lists below are by no means exhaustive but are an attempt to provide a framework for activities which fall into the category of unacceptable use.

3.3.4.1 System and Network Activities

The following activities are strictly prohibited. Should any you have knowledge of misuse, you must notify your manager or Human Resources immediately.

- You will not export software, technical information, encryption software, or technology in violation of international or regional export control laws. Users understand this is illegal. The CISO will be consulted prior to the export of any material that is in question.

- You will not take actions that interfere with the proper functioning or the ability of others to make use of Acrisure's networks, computer systems, applications and data resources including port scanning or security scanning unless approved by the CISO.
- You will not introduce malicious programs onto the network, servers, workstations, or mobile devices (*e.g.*, viruses, worms, Trojan horses, e-mail bombs, etc.).
- You will not reveal account password(s) to others or allow the use of account by others. This includes family and other household members when work is being done at home as well as use by other Acrisure employees.
- You will not use an Acrisure computing asset, system, or network to engage in procuring or transmitting material that could be considered harassment as defined in the Acrisure Code of Conduct or is in violation of sexual harassment or hostile workplace laws.
- You will not make fraudulent offers of products, items, or services originating from any Acrisure account.
- You will not make statements about warranty, expressly or implied, unless it is a part of normal job duties.
- You will not cause or effect a security breach or disruption of Acrisure systems, storage, networks, or communications.
    - Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access.
    - Disruption includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- You will not circumvent User authentication or security of any host, network, or account unless this activity is a part of User normal job/duty.
- You will not intentionally interfere with or deny service to any Acrisure or customer network, system, or cause a denial of service attack.
- You will not provide information about, or lists of, Acrisure employees to outside parties unless part of official job duties.
- You will not jailbreak or root a mobile device configured for access to Acrisure data or networks.
- You will not use alternate proxy servers, VPN, or any other means to bypass Acrisure filtering or monitoring.
- You will not use an Acrisure computing asset to procure or transmit content that is sexually explicit, constitutes pornography, or illegal.
- You are not permitted to install wireless access points or modems in the Acrisure environment without Acrisure IT's written authorization.
- You are not allowed to disengage or change the anti-virus or device management software installed on any device used to connect to Acrisure's network unless authorized in writing by the Acrisure IT Security team.
- You are not permitted to store an Acrisure work product on any device or in any system other than on an Acrisure issued device, authorized BYOD or on the Acrisure network. All Acrisure work product remains the property of Acrisure regardless of device, system, or network.
- You will not download or send confidential information to (a) any personal email accounts; (b) any personal account on a third-party data sharing site (Box, etc.); or (c) any media (such as a flash drive).

3.3.4.2 Email and Communications Activities

- You will not send unsolicited email messages, including the sending of spam or other advertising material to individuals who did not specifically request such material from any Acrisure account.
- You will not engage in any form of harassment via email, instant messaging, telephone, or texting, whether through offensive or inappropriate language, frequency, or size of messages. Acrisure is an equal opportunity employer and prohibits discrimination as described above. Acrisure assets, including authorized BYOD devices, may not be used to spread or convey discriminatory, violent, or offensive material.
- You will not spoof or forge email header information, unless part of a security audit.
- You will not create or forward "chain letters", "Ponzi" or other "pyramid" schemes of any type on any Acrisure asset or from any Acrisure account.
- You should not open an email attachment from an individual or source User does not recognize, and User should “Phish Alert Report” button notify Acrisure IT or forward the suspicious email to security@acrisure.com for review.
- You will use appropriate security measures when using publicly shared computers, smartphones, or tablets to access Acrisure computers, systems, networks, or cloud infrastructures and only do so when necessary.

3.3.4.3 Social Media Activities

Acrisure endorses the use of social media and networking to enhance communication, collaboration, and knowledge. We respect your rights of personal expression through social media and networking mediums – we must also protect our confidential and proprietary information and business interests. This policy, therefore, provides rules and guidance for you regarding your use of social media and other electronic communications tools such as blogs, personal websites, podcasts, e-mail, and message boards.

For purposes of this policy, the term “social media and networking” includes viewing, visiting, and/or using various Internet websites, tools, and applications, including but not limited to Facebook, Twitter, Linked-In, Instagram, Snapchat, etc.

Since social media and networking activities must not interfere with your job performance and work commitments, this policy pertains to social media and networking activities that are:

- Performed during and off regularly scheduled working hours and days
- Performed on and off the Company’s premises
- Performed on the Company’s computer, phone, or other electronic equipment (e.g., computers, iPhones, etc.)
- Performed on an your or third party’s computer, phone, or other electronic equipment.

All use of social media by you, whether for business or personal activities, is subject to Acrisure’s policies and contractual obligations. If your post would violate any of Acrisure’s policies in another forum, it will also violate them in an online forum. Do not use social media to disclose confidential or proprietary Acrisure information, harass, or discriminate against fellow employees, defame or disparage Acrisure or fellow employees, or violate any other Acrisure policy. You must also not use social media in a false or

misleading way; for example, by claiming to be someone other than yourself or by creating an artificial "buzz" around Acrisure's business or products.
You are expected to comply with the following rules when viewing, visiting, and/or using social media and networking websites, tools, and applications:

- **Transparency**. When promoting our services on social media platforms, identify yourself as an employee of Acrisure clearly and conspicuously.
- **Pseudonyms**. You may use pseudonyms for privacy, but not to circumvent this Policy, or to mislead readers about their Acrisure affiliation.
- **Endorsements**. If you are endorsing Acrisure's services, then you must plainly disclose their employment with us. You, however, should not use social media and networking mediums to conduct unauthorized marketing or public relations. Only those persons officially designated by Acrisure are authorized to speak on behalf of us in this regard.
- **Disclaimer**. If you disclose your full name and employment at Acrisure, and express views on political, religious or other matters of public concern, then you must state that the views are not necessarily endorsed by Acrisure. That statement must live in the "Profile," "Information," "About Me," or similar platforms available on social media or networking websites. The following examples are appropriate disclaimers:
  - "My Tweets are my own and are not endorsed by my employer."
  - "The postings on this site are my own and do not necessarily represent the Company's positions, strategies or opinions."
- **Unauthorized Use.** You may not claim to act as an official representative or agent of the Company when engaging in social media and networking activities. You may also not falsely create the impression that you have expertise about our services or business if you do not have appropriate expertise.

Additionally, we trust that you will exercise good judgment when participating in social media and networking activities. You, therefore, must comply with the following guidelines when viewing, visiting, and/or using social media, networking, and other Internet websites:

- **Respect copyright and fair use laws**. You should know that copyright and trademark laws may restrict the use and copying of material belonging to the Company and/or others when they use social media or post on the Internet. You may not violate the intellectual property or privacy rights of the Company or others under any circumstances.
- **Protect confidential and proprietary information**. You may not disclose any trade secrets, confidential information, or proprietary information belonging to the Company or its clients to individuals outside the Company. This includes, among other things, disclosing business plans, strategies, and financial information, and future business prospects. The Company reserves the right to request that you temporarily or permanently suspend any communications that disclose trade secrets and confidential and proprietary information.
- **Respect the Company's Equal Employment Opportunity policies**. Remember that the Company is a diverse organization employing employees who reflect a diverse set of customs, values and points of view. Accordingly, you may not use social media or networking mediums to post or display comments about colleagues, coworkers, supervisors, clients, and Acrisure that are vulgar, obscene, threatening, intimidating, harassing, or a violation of our policies against discrimination, harassment, or hostility on account of any characteristic protected by applicable federal, state, and local laws.

- **Not Engage In Other Inappropriate Conduct**. You must refrain from blogs or posts that are defamatory or libelous or support a competitor of the Company or its affiliates.

Nothing in this Policy shall be deemed to limit employees' rights under applicable federal, state or local law, including the National Labor Relations Act.

3.3.5 Password Management

Passwords are an instrumental part of a strong security infrastructure. You should:

- Use unique User identification to logon to any Acrisure application or network.
- Abide by the Acrisure password requirements.
- Never write down passwords and use the Acrisure provided password management platform if provided.
- Immediately change a password if it has become known and notify the Acrisure IT Security team and your leader within 24 hours, or, if possible, sooner.

3.3.6 Physical Access

- To adequately protect Acrisure buildings and infrastructure you should:
- Be aware of who is in their area before accessing Sensitive Data or non-public information. Sensitive Data or non-public information displayed on a monitor should not be viewable by the public or escorted visitors.
- Ensure that visitors sign in upon arrival and sign out at departure at the entrance to Acrisure buildings. The logs should ask for the visitor's name, the firm represented, and the employee authorizing physical access.
- Ensure that the visitors are provided badges which clearly reflect that they are visitors to the facility. Badges should have "visitor" clearly printed on them. Users should ensure that the visitor returns the badge at the end of the visit.
- Escort visitors.
- Not share their badge or building access card or allow another to do so.
- Report the loss of a badge or access card to the Acrisure Facilities department as soon as possible after realizing the badge or access card is missing.
- Promptly report any physical security incidents to Facilities and the CISO.

3.3.7 Intellectual Property Rights

- You will not access copyrighted material for which you do not have ownership or license. Violating copyright laws is prohibited, including, but not limited to, illegally duplicating or transmitting copyrighted material; for example, pictures, music, video, and software from various types of peer-to-peer file-sharing networks.
- Exporting or importing software, technical information, encryption software, or technology must never be in violation of international or regional export control laws.
- You will not violate the rights of any person or Acrisure protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to,

the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by you or Acrisure.

- You will not engage in the unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted video, or the installation of any copyrighted software for which you or Acrisure does not have an active license.

3.3.8 Enforcement

In addition to any legal remedies Acrisure may have, and any disciplinary action with may be taken with respect to your employment, where illegal activities are suspected, Acrisure will report such activities to the applicable authorities. Please see the Company's Acceptable Use Policy, which can be found Here.

3.4 Global Privacy Policy

We are committed to adhering to applicable data privacy laws and regulations of the United States, the United Kingdom, the European Union and other jurisdictions in which we operate. Acrisure has created and implemented a Global Privacy Policy, which can be found Here.

3.5 Records Management Policy

We are committed to ensuring good data hygiene and compliance with all applicable laws and regulations to guard against accidental or improper destruction or dissemination of records. The Company will prepare and maintain complete, accurate, reliable and organized records. We will handle confidential records securely and as required by applicable law, including appropriate retention, use and disclosure limitations, notice requirements and other requirements under applicable law. The Company has created and implemented a standard and systematic records management program. For details regarding this program, please refer to Acrisure's Records Management Policy and Records Retention Schedule (U.S.), which can be found Here.

4 Conduct of Acrisure's Business

4.1 Acrisure's International Anti-Corruption Compliance

We recognize the significant harm that corruption poses for the markets in which we operate. As a result, we are committed to the highest prevailing domestic and international anti-corruption standards. We do not pay bribes or engage in corruption either directly or through third parties. Our personnel must comply with the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act 2010 and anti-corruption laws of other countries where we operate. For additional detail, see Acrisure's International Anti-Corruption Compliance Policy, which can be found Here.

4.2 Gifts and Hospitalities

Fostering goodwill and positive business relationships through the provision of gifts, meals, entertainment, hospitality and travel ("G&H") is considered a normal part of doing business. Such G&H must be reasonable and bona fide. It is especially important that G&H involving suppliers, customers, or others having business dealings with us does not create an actual or apparent conflict of interest or violate

applicable law. The Company has adopted a Gifts and Hospitalities Policy, which can be found Here, to provide guidance with respect to G&H.

The Company's U.S. Political Activity Policy, which can be found Here, provides additional guidance with respect to any G&H involving U.S. federal, state and local government officials.

4.3 ANTI-MONEY LAUNDERING

Money laundering is using money in a way that disguises its true source. It can be done in many ways and some industries, such as the insurance industry, are particularly vulnerable to laundered money. For example, if a person purchases an insurance product with "dirty" money (*i.e.*, money from illegal acts) and then cancels it, depositing the refund check may make the "dirty" funds appear to be "clean."

Applicable laws make it a crime to engage in money laundering. It also is a crime to "aid and abet," or knowingly help, someone who is engaged in money laundering. Please see Acrisure's Global AML Policy, which can be found Here.

4.4 SANCTIONS

Acrisure expects all personnel to comply with its Sanctions Compliance Policy and U.S. Sanctions Compliance Policy, as applicable, each of which can be found Here, and applicable sanctions at all times. Although personnel are not expected to master applicable sanctions, it is important that they know when to seek advice from supervisors or other appropriate persons. Failure to comply with applicable sanctions may result in civil, administrative and criminal penalties, including, but not limited to, freezing or blocking of assets, monetary fines, damage to the Company's reputation, or limitation on the Company's business activities. Violations can also result in imprisonment. Failure to comply with Acrisure's Sanctions Compliance Program or with applicable sanctions is grounds for disciplinary action, up to and including termination. Please also see Acrisure's Screening, Assignment and Recusal Policy, which can be found Here.

4.5 POLITICAL ACTIVITY

The Company encourages the interests of its employees in the governmental process. However, it is very important that any participation in the governmental process be undertaken as an individual – not as a representative of the Company.

The Company sets forth in its U.S. Political Activity Policy, which can be found Here, mandatory minimum requirements regarding compliance with regulation of the Company's lobbying, political outreach and bestowing of gifts and entertainment to U.S. public officials and entities in local jurisdictions, the states, in Congress and the federal executive branch. Provisions relating to non-U.S. officials are set forth in the Company's International Anti-Corruption Compliance Policy, which can be found Here.

Failure to comply with applicable laws, even if that failure is inadvertent and caused by lack of awareness of the law, could result in a legal violation, civil and/or criminal penalty, the loss of government business and reputational risk for the Company.

5 WAIVERS AND REVISIONS

Waivers of or exceptions to this Code will be granted only in rare circumstances. Waivers or any other amendment to this Code will be considered by the Company's Chief Executive Officer, together with the Chief Legal Officer.