AIRIP Code of Conduct

AIRIP is committed to the following values and practices:

Code of Conduct for Risk Intelligence Professionals

- We will uphold the brand and reputation of the organizations for whom we work
- We will not misrepresent ourselves in person or online
- We will abide by all applicable laws
- We will analyze qualitative and quantitative data in an objective way, in order to provide thoughtful, thorough, and unbiased analysis
- We will promote this Code of Conduct within our teams and organizations, with our third-party vendor providers, and with our colleagues across the profession
- We will speak highly of this profession, and increase the reputation of intelligence analysis
- We will adhere to the policies and procedures of the organizations for whom we work
- We will foster an ethical and responsible risk intelligence community

AIRIP upholds this standard as a best practice for its members and others in the profession, and asks that its members adhere to the principles outlined above. AIRIP reserves the right to revoke/terminate membership at any time if this is not upheld by a member.

This Code of Conduct may be used as a formation and reference document for codes of conduct in the organizations where our members work.

FAQ

This FAQ has been developed to examine some scenarios and circumstances that may require additional clarification under the AIRIP Code of Conduct.

What is the AIRIP Code of Conduct and what does it mean?

The AIRIP Code of Conduct is a high professional standard that we ask our members to abide by and uphold. The profession of risk intelligence is inherently difficult to define, as the nature of the work is sensitive and generally not talked about. We aim to provide a framework for new and established analysts and teams to use as they develop and mature their intelligence programs. With this Code of Conduct, we would like to provide guardrails for teams as they make decisions within their programs with regard to collecting and disseminating information. We also want to provide a professional standard that our members can use when speaking with others in their organizations or externally about how and why information is collected and disseminated in certain ways.

AIRIP believes that this standard is critical to the credibility of the profession and we ask our members to abide by it, uphold it, apply it to their own programs and share with others in the profession. All members of the Board are asked to adhere to it strictly.

Who should use this professional standard?

This Code of Conduct is a professional standard for the Association of International Risk Intelligence Professionals (AIRIP) members and prospective members. It can also be used by others in the field of risk intelligence, including professionals with duties such as intelligence analysis, political risk analysis, business strategy formation, mergers and acquisitions research and strategy, travel security analysis, security operations center professionals, crisis management, risk assessment, and other diverse duties.

Can you provide more information about specific collection efforts?

Intelligence collection can mean a lot of different things. Risk Intelligence analysts most often work with publicly available or open source information. Open sources include:

- Media: newspapers, magazines, radio, television, and computer-based information
- Web-based communities and user-generated content: social-networking sites, video sharing sites, wikis, and blogs
- Public data: government reports, official data such as budgets, demographics, hearings, legislative debates, press conferences, speeches, marine and aeronautical safety warnings, environmental impact statements, and contract awards.
- Professional and academic: conferences, professional associations, academic papers, and subject matter experts

This type of risk intelligence collection is not considered covert or clandestine collection. AIRIP will not tolerate any member who breaks the law in collecting risk intelligence information. AIRIP requires that its members act and perform research in ways that uphold the brands and reputations of their organizations.

Some specific examples include:

- **Anonymizers**: Conducting web research using an anonymizer (a computer application that hides the origin of your IP address) is generally acceptable within this Code. With an anonymizer you provide your team, analysts, and company with a level of security by not sharing your location or IP address. With this type of service you are not misrepresenting who you are, as you are not providing any information about who you are, or are not.
- **E-mails for the purpose of information collection:** AIRIP generally believes that the collection of information through the use of e-mail addresses through a host other than your organization is acceptable and falls within this standard. That said, the e-mail address should be generic, and should not represent the identity of a real person. These e-mails may be used to collect publicly available data from open sources (for example: a general e-mail newsletter for an organization, or a public Facebook page), but not from password protected websites, or through e-mail interaction where you may have to hide your true identity.
- **Face-to-face or phone/e-mail conversations with sources, as well as online interactions via e-mail and social media, among other mediums:** AIRIP members should accurately identify themselves in interactions with all sources, targets, vendors, and others. Collection of data and information only available

through close personal relationships if that relationship is made under false pretenses, or collection through password protected sites, if the credentials are gained under false pretenses does not withstand this test.

- If interaction with a threat actor or group is necessary, members should work with their legal departments and/or law enforcement to understand which/if any measures should be taken to protect themselves and their identity. We consider threat actors to be persons involved in malicious activity with \intent to harm a person, organization, or organization's reputation.

Are the rules different for any third-party providers or vendors that we use?

No, for the most part. In almost all cases, AIRIP members should hold their vendors and third-party providers to the values and practices laid out in this Code of Conduct and FAQ. We do not ask or pay another person to do the illicit or prohibited work for us. AIRIP encourages you to use your own collection methods, as well as vendor collection, as far as you can go within the professional standard. We recommend that you develop your network of sources, and make your analytical judgement based on the information available. In most cases, information that may have been obtained unethically does not provide enough incremental value that it is worth risking your own personal or organizational reputation to obtain.

For areas where you suspect there is potential criminal conduct being committed, AIRIP suggests that you contact law enforcement and work with your legal department in determining an appropriate response. An example of this may include using a third-party to gain information on potential cyber-threats or vulnerabilities for your organization. Vendors vary greatly in the methods they use to gain information. Some third-party providers may be using methods that are contrary to this Code of Conduct to gain access to forums and dark web areas. We recommend that you work closely with your legal department and/or organization's ethics officer to clarify which type of collection methods are acceptable in your organization.

Can I access sensitive or classified law enforcement or government information?

Some members of AIRIP may have security clearances that allow them access to see classified information in the U.S. and other countries. In the case that a cleared individual reads or receives classified government information, that individual must protect that information according to proper handling requirements and applicable federal or state law. This often means that the information, its sources, and the methods used to obtain it cannot be shared further or incorporated into any analysis produced by the AIRIP member.

Additionally, as a condition of holding a security clearance, cleared individuals agree that they will not attempt to access information above their current security clearance level. This condition includes the agreement to not access or use information that has been made public through leaks or breaches, such as Wikileaks.

Finally, government personnel who move into a private sector capacity may use their business and government connections to gather information that is publicly available,

but that information may not include material or collection methods to which they are no longer cleared to access.

How does this fit with my organization's code of ethics and/or code of conduct?

In the spirit of fostering an ethical and responsible risk intelligence community, gathering
risk intelligence and producing analytical reports should be done in accordance with this Code of Conduct, as well as the policies of your organization – whichever is stricter.

Which functional areas should I work with in my organization to understand how this code of Conduct applies?

The following are some examples of stakeholders within your organization to include when examining how this Code of Conduct applies to your risk intelligence program: legal department, competitive intelligence, compliance, ethics, security, and human resources.

How are alleged violations of this code of conduct reviewed, and what are the ramifications of non-compliance?

If AIRIP receives information that may indicate that a member has violated this Code of Conduct, the member will be contacted by AIRIP staff and asked to submit a statement outlining the situation and any additional information addressing the allegation. The Board of Directors of AIRIP will then evaluate that information, and may ask to speak with the member, to determine if a violation has occurred. If the Board finds that the member has violated this Code of Conduct, the Board will revoke the member's AIRIP membership, and the member will forfeit any member dues paid.

Members removed from AIRIP will be eligible to reapply after a period of six months.