TLP:WHITE

EthicsfIRST

Ethics for Incident Response and Security Teams

Members of incident response and security teams (Teams) have access to many digital systems and sources of information. Their actions can change the world. As a member of this profession, a Team member must recognize responsibility to their constituency and to other security professionals, as well as to wider society. The individual must also recognize their responsibility to their own well-being.

EthicsfIRST is designed to inspire and guide the ethical conduct of all Team members, including current and potential practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. This framework includes principles formulated as statements of responsibility, based on the understanding that the public good is always the primary consideration. Each principle is supplemented by guidelines, which provide explanations to assist computing professionals in understanding and applying the principle.

The duties are introduced below but are not in order of importance. These duties should not be seen as absolute requirements, but rather as stated in the IETF RFC2119 for the definition of "SHOULD":

> "This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore particular [duties], but the full implications must be understood and carefully weighed before choosing a different course."

For more information on how to deal with possible dilemmas, see *Appendix A*.

Duty of trustworthiness

Trust is the basis of many relations between Teams and is often required before meaningful exchange of information can occur. The FIRST community is built on this trust, and it can only continue to function in this way if there is a reasonable level of trust between Teams.

Trustworthiness means that Team members should only: 1) enter into commitments that they can keep, 2) behave predictably towards other Teams (e.g., respect the TLP standard), and 3) uphold the trust relationship they have with other Teams.

The trust relationship should be initially assumed and transitive, i.e., Trust on First Use (TOFU), and enable trust for Teams that are trusted by other Teams.

Duty of coordinated vulnerability disclosure

Team members who learn of a vulnerability should follow coordinated vulnerability disclosure by cooperating with stakeholders to remediate the security vulnerability and minimize harm associated with disclosure. Stakeholders include but are not limited to the vulnerability reporter, affected vendor(s), coordinators, defenders, and downstream customers, partners, and users.

Team members should coordinate with appropriate stakeholders to agree upon clear timelines and expectations for the release of information, providing enough details to allow users to evaluate their risk and take actionable defensive measures.

Duty of confidentiality

Team members have a duty to maintain confidentiality where appropriate. Requests to keep certain information in confidence may be made explicit, for example, with the Traffic Light Protocol (TLP). Team members should respect such requests whenever possible. If it is not possible to keep information in confidence, for example, due to conflicts with the requirements of local laws, contracts, or a duty to inform, the Team member should inform the information owner of this conflict immediately.

Some duties of confidentiality are based on laws, regulations, or customs. If, during an incident response, some parties are bound by or expect confidentiality based on such considerations, they should do their best to make these expectations explicit in advance. All parties should then abide by the above expectation to maintain explicit requests to keep information in confidence when possible.

Duty to acknowledge

Teams receive information from many different sources: researchers, customers, other Teams, government entities, etc. Team members should respond to inquiries in a timely manner, even if it is only to confirm that the request has been received. When possible, Team members should set expectations for the next update.

Duty of authorization

Team members have a legitimate need and right to understand their areas of responsibility, acting only on systems that they are authorized to access. Team members need to be aware of how their actions may affect their constituents and ensure they do not cause additional harm while performing their duties. Where possible, constituents should be consulted before changes are made to their systems.

Duty to inform

Team members should consider it their duty to keep their constituents informed about current security threats and risks. When Team members have information that can either adversely affect or improve safety and security, they have a duty to inform relevant parties or others who can help, with appropriate effort, while duly considering confidentiality, privacy laws and regulations, and other obligations.

Duty to respect human rights

Team members should be aware that their actions may impact human rights of others through the sharing of information, a possible bias in their actions, or an infringement of property rights. Team members have access to a wide range of personal, sensitive, and confidential information in the course of handling incidents. This information should be handled in a way to uphold human rights.

During incident handling, responders should not act in a biased manner and should do their utmost to eliminate bias from their processes and decision-making, either performed by responders or built into algorithms.

For the purpose of this principle, the notion of "property" (UN Declaration of Human Rights: Article 17) includes intangibles such as intellectual property, as well as ideas and concepts in general, regardless of whether they are legally protected (e.g., patented).

Duty to Team health

Teams have a responsibility to continue to provide the services they have promised their constituents. This responsibility includes the physical and emotional health of the Team.

In order to both respect as individuals the members who make up a Team and enable the long-term viability of sustaining an adequate level of service, a Team should strive to maintain a healthy, safe, and positive work environment that supports the physical and emotional health of (all) its members. In order to respond to a crisis, "normal" operations should support emotional health and stress reduction.

Duty to Team ability

Incident management is an evolving subject that Team members should continually study. A Team should provide resources to its members for them to study, apply, and advance technological and scientific knowledge within their area(s) of responsibility. Training or educational CPE/CEU credits may contribute, but mere compliance exercises are insufficient to fulfil this duty. A Team should maintain sufficient technological infrastructure so as to enable its services, including adequate measures to protect that infrastructure from interference by outside parties.

Duty for responsible collection

Data collection is necessary for incident response, but a balance should be struck between the goal of incident response and respecting the data stakeholders.

During an investigation, the amount of information needed to collect may change. While progressing through an incident, Team members should adjust what they are collecting as the need changes. Data not directly relevant to an incident and its remediation should be excluded from reporting.

Collected and extracted data must be handled in accordance with applicable laws and respect of user privacy. Permission should be sought before collecting and processing data under the control of a data owner. Applicable law and regulations in handling data should be respected.

Data that may help other response Teams in their efforts related to other incidents should be made available to them, possibly in redacted form. Information that is confidential and proprietary should only be made available with appropriate protections.

Before sharing data with third parties for mitigation, the risks should be weighed against the benefits. Data should only be shared if the benefit clearly outweighs the risks. Sensitive data should be stored in a way that it can easily be destroyed after an incident has been closed. Collected data should be safely destroyed in accordance with data retention policies.

Duty to recognize jurisdictional boundaries

Team members should recognize and respect the jurisdictional boundaries, legal rights, rules, and authorities of the parties involved in activities related to incident response.

Laws, regulations, and other legal issues, such as those related to privacy protection or data breach notifications, may differ between the involved jurisdictions. Jurisdictional boundaries may be determined by the involved parties physica l locations, such as their countries or domiciles, as well as by other factors concerning those parties. Even within a single country, laws and regulations may differ between political regions (e.g., between individual states in the USA) or between different businesses, industries, or sectors within that nation (e.g., healthcare, financial services and government facilities). National CSIRTs may have designated responsibilities and/or authority for activities involving constituents within their own jurisdiction, and they may also collaborate with or "hand off" information and activities to other entities that have authority for jurisdictions that cross boundaries.

Team members should be aware of key issues that affect the jurisdictions involved, including but not limited to privacy regulations or data breach notification requirements. Because cybersecurity and privacy laws and regulations evolve and continue to be updated worldwide, it is advisable to consult with informed legal counsel for guidance whenever issues involve multiple jurisdictional boundaries.

Duty of evidence-based reasoning

Teams should operate on the basis of verifiable facts. When sharing information, such as indicators of compromise (IOCs) or incident descriptions, Team members should provide evidence and scope transparently. If this is not possible, the reasons for not sharing this evidence and scope should be given with the information.

Team members should refrain from spreading or sharing rumors. Any hypothesis should clearly be identified as such.

Transparent evidence and reasoning processes are important even in the case of automated sharing, e.g., during automated sharing of large amounts of information. In this case, a description of the data mining process should be communicated at an intelligible level of detail.

Appendix A
Dealing with Dilemmas

Team members may frequently find themselves in a position where no action seems to satisfy all of the ethical principles. In such a situation, a choice must be made as to which principles to prioritize. In this situation, incident handlers are encouraged to reflect on which stakeholders may be affected by their actions and how, preferably in a discussion with a colleague. As a rule, the solution that minimizes the infringement of this ethical framework should be chosen. At times, this might not be possible, e.g., due to external pressures. In such a situation, it is recommended to proceed, making note of the ethical dilemma, possibly under protest.