TLP:WHITE

事故响应与安全团队论坛（FIRST）道德和职业操守准则草案

事故响应与安全团队（简称安全团队）的成员可以访问大量数字系统和信息源，其行动可以改变世界。作为这一行业的从业者，安全团队成员必须认识到他们对其服务对象、其他安全专业人员以及社会各界的责任。而每位个人也必须认识到他们对自身利益负有的责任。

本准则旨在激励和指导所有安全团队成员的道德行为，其中包括在职和潜在的从业者、教师、学生、有影响人士以及所有以有效方式使用计算技术的人员。本准则基于对公共利益始终是首要考虑因素的理解，包括了作为责任声明制定的原则。每项原则都得到导则的补充和说明，以帮助计算机专业人员理解和应用该原则。

各项责任介绍如下，但并未按其重要性排序。这些责任不应被视为绝对要求，而应采用 IETF（互联网工程任务组）RFC 2119 中对“应”（SHOULD）的定义：

> “在实际环境中有可能存在正当的理由对一特定条款不予理会，但是，在选择不同的做法之前应充分理解和小心权衡全部含义。”

有关如何处理可能出现的困境的更多信息，请参见附录 A。

守信责任

信任是安全团队之间诸多关系的基础，通常是开展有意义的信息交换的先决条件。事件响应与安全团队论坛（FIRST）群体以这种信任为基础，只有安全团队之间达到合理程度的互信，才能继续以这种方式运行。

可信度意味着安全团队成员只应：1）做出他们能够遵守的承诺，2）对其他安全团队施以可预见的行为（如遵守 TLP 标准），以及 3）维护他们与其他安全团队之间的信任关系。信任关系应首先假定并具有传递性，即首次使用信任（TOFU），并允许受信于其他安全团队的安全团队获得信任。

协调漏洞披露的责任

察觉漏洞的安全团队成员应与利益攸关方合作，协调漏洞披露工作，修复安全漏洞，并将与披露相关的危害降至最低。利益攸关方包括但不限于漏洞报告人、受影响的供应商、协调人、维护者以及下游客户、合作伙伴和用户。

安全团队成员应与适当利益攸关方协调，就信息发布的明确时间表和预案达成一致，提供足够的细节，使用户能够做出风险评估，并采取可操作的防范措施。

保密责任

安全团队成员负有酌情保密的责任。可以像交通信号灯协议（TLP）那样明确提出对某些信息实行保密的请求。安全团队成员应尽可能尊重这些请求。如果由于与当地法律、合同或告知义务的要求相抵触而无法实行信息保密，安全团队成员应立即将此利害冲突告知信息拥有者。

一些保密责任以法律、法规或习惯为依据。如果在事故响应过程中，一些参与方基于此类考虑而遵循或期待保密规定，他们应尽最大努力提前明示这些期望。之后所有各方均应遵循上述期望，尽可能坚持提出明确的信息保密要求。

确认责任

安全团队从研究人员、客户、其他安全团队、政府实体等许多不同来源接收信息。安全团队成员应及时回复询问，即使只是对请求收悉的确认。如果可能，安全团队成员应该设定预期的下一次更新。

授权责任

安全团队成员拥有了解其职责范围的合法需求和权利，并只能通过他们有权访问的系统采取行动。安全团队成员必须意识到其行动对其服务对象可能造成的影响，并确保他们在履行职责时不会造成额外伤害。应向受影响的利益攸关方说明这些行动可能带来的后果。在对其系统进行更改之前，应尽可能征求服务对象的意见。

告知责任

安全团队成员应将 shi 其服务对象了解当前的安全威胁和风险视为自己的责任。当安全团队成员掌握的信息可能对安全和安保产生不利影响或使二者得到改善时，他们均有义务通过适当努力告知相关方或其他能够提供帮助的人，同时充分考虑到保密、隐私法律法规或其他义务。

尊重人权的责任

安全团队成员应该意识到，他们的行为可能会因为信息共享、行动中可能存在的偏差或对财产权的侵犯，令他人的人权受到影响。在事故处理过程中，安全团队成员可以接触到广泛的个人、敏感和机密信息。应以维护人权的方式处理这一信息。

在事故处理过程中，响应者不应偏颇行事，而应尽最大努力消除其流程和决策中的偏差，无论它存在于响应者的履职过程还是内置于算法之中。

就这项原则而言，“财产”的概念（《联合国人权宣言》第 17 条）包括无论是否受到法律保护（如专利）的知识产权以及通常的思想和概念等无形资产。

安全团队的健康责任

安全团队有责任持续向其成员提供承诺的服务。这一责任关系到安全团队的身心健康。

为了尊重安全团队成员的人格和能够长期维持适当的服务水平，安全团队应努力维持一个健康、安全和积极的工作环境，以保证（所有）成员的身心健康。为了应对危机，“正常”的工作应有助于情绪健康和缓解压力。I

团队的能力建设责任

安全团队成员应该不断研究事故管理这一持续变化的主题。安全团队应向其成员提供资源，以便他们在各自的职责范围内研究、应用和推进科技知识。培训或教育继续职业教育 (CPE) /继续教育 (CEU)学分可能有所帮助，但仅进行合规练习不足以履行这一职责。安全团队应为其服务提供维持充足的技术基础设施，包括为保护该基础设施免受外方干扰的适当措施。

负责任的数据采集责任

数据采集是事故响应的必需，但是应该在事故响应的目标与尊重数据利益攸关方之间达成平衡。

在调查过程中，需要采集的信息量可能会有变化。在事件处理的过程中，安全团队成员应该根据需求的变化调整其采集内容。

不直接与事故及其补救措施相关的数据应被排除在报告之外。

须根据适用法律和以尊重用户隐私的方式，处理采集和提取的数据。只有在获得许可后，才能对数据所有者掌握的数据进行采集和处理。应遵守适用的数据处理法律和法规。

或可以编辑后的方式，向其他响应团队提供可能有助于他们处理其他事故的数据。机密和专用信息只能在有适当保护的情况下提供。

在为缓解风险与第三方共享数据之前，应权衡益处与风险。只有当益处明显大于风险时，才可共享数据。应存储敏感数据，以易于事故结束后予以销毁。应根据数据保留政策，安全地销毁采集的数据。

承认管辖范围的责任

全团队成员应承认并尊重参与事故响应相关活动各方的管辖范围、法律权利、规则和权限。

法律、法规和与隐私保护或数据泄露通知相关的其他法律问题，可能会因涉及的管辖区而异。管辖范围取决于相关方的国家或居住地等地理位置以及与之相关的其他因素。即使在一国之内，法律和法规也可能因行政区域（如美国各州）或国内不同企业、行业或部门（如医疗保健、金融服务；政府设施）而有差异。国家计算机安全事件响应团队（CSIRT）可能对涉及其管辖范围内成员的活动负有既定的责任和/或权限，而且它们也可能与拥有跨境管辖权的其他实体合作，或向这些实体“移交”信息和活动。

安全团队成员应了解影响相关管辖区的关键问题，包括但不限于隐私法规或数据泄露通知要求。由于网络安全和隐私法律法规在全球范围内的不断发展和更新，每当问题涉及多个管辖范围时，建议咨询知情的法律顾问以获得指导。

循证推理的责任

安全团队应该在可查证事实的基础上运作。当共享诸如妥协指标（IOC）或事故描述等信息时，安全团队成员应该透明地提供证据和范围。如果做不到这一点，就应在提供信息的同时，提出不分享这一证据和范围的理由。

安全团队成员应避免传播或散布谣言。应明确标明所有假设。

即使在自动共享的情况下，例如在自动共享大量信息的过程中，也必须有透明的证据和推理过程。在这种情况下，对数据挖掘过程的描述应以可理解的详细程度加以通报。

附录 A

应对困局

安全团队成员经常会发现自己处于似乎无论采取任何行动都无法满足所有道德原则的境地。在这种情况下，必须做出优先考虑哪些原则的选择。就此，应鼓励事故处理者最好通过与同事的探讨，思考其行动会对哪些利益攸关方产生多大程度的影响。通常，应选择能够最少违背本准则的解决方案。有时，会因外部压力无法做到这一点。在这种情况下，建议在将道德困局记录在案的同时，可能需顶着抗议继续努力。