2.

**Nontechnical skills**

CSIRT work is service-based. Thus, all CSIRT staff must demonstrate diplomacy and communicate competency in interactions with constituents.

* **Willingness to follow instructions.** Staff should be familiar with defined CSIRT procedures and policies and the importance of upholding them.
* **Communication.** Staff should demonstrate effective written and interpersonal communication skills necessary to fulfill duties such as documenting incident reports or presenting technical briefings.
* **Collaboration.** Due to the cooperative nature of the CSIRT structure, members must be committed team players to ensure collective morale, productivity and agility.
* **Time management.** Staff should understand how to use provided criteria to prioritize various CSIRT activities and determine when to ask for help from management.
* **Analytical reasoning.** CSIRT staff need to think out of the box to anticipate attacker techniques and problem-solve in potentially volatile situations.
* **Stress management.**The demanding nature of incident response and risk of [security staff burnout](https://www.techtarget.com/searchsecurity/post/6-ways-to-prevent-cybersecurity-burnout) warrant special attention to managing stress, as well as work-life balance.
* **Continuous learning.** Incident response is a constantly changing area of expertise. Thus, CSIRT members must be inquisitive people and embrace opportunities to further their skills through training, certification or mentorship.

3.

<https://www.logsign.com/blog/what-is-csirt-what-are-csirt-roles-and-responsibilities/>

<https://hitachi-systems-security.com/key-roles-and-responsibilities-for-your-incident-response-team-3-5/>

1.