**Ethical Implications of Cybersecurity Analyst Access**

Andrew Burbage

Principles of Cybersecurity

Dr. Sun

January 22, 2026

The question of granting a cyber security analyst access to all systems under an organization is a question of reducing risk, using/adhering to authorizations, and choosing a candidate that isn't risky. The answer is both yes and no. An analyst should have access to all pertinent systems so that they can identify and mitigate risks as well as identify and counter attacks. Both the IEEE and ACM code of ethics highlight this. In section 2.9 of the ACM code of ethics they call for a "robust security" implementation that protects sensitive data and vital functions. (Association for Computing Machinery [ACM], 2018) Section I subsection 1 of the IEEE code of ethics asserting that risks and threats should be reported "promptly". (Institute of Electrical and Electronics Engineers [IEEE], 2020) This is the yes in that access is necessary for a robust security structure and for prompt reporting and reaction. However, the no comes in with not granting access with a wanton disregard for the risks that comes with a privileged account like this. The ACM code of ethics addresses this as well under section 2.9 asserting that restriction is a right and adherence to this restriction is the only ethical path forward. (Association for Computing Machinery [ACM], 2018) Essentially, with all systems it is allowed and wise to restrict access to limit malicious actors both internal and external. In this case that means that while the analyst should be given access to protect against external threats, their access should be restricted to only what is necessary so as to prevent internal threats from their privileged status. Lastly, an ethical choice on granting the aforementioned limited access is heavily dependent on choosing an ethical candidate for such a position. Section I of the IEEE code of ethics touches on this under subsections 3 and 4. Subsection 3 asserts that to avoid

conflicts of interest, another way to frame this is to avoid a candidate that is likely to act maliciously out of self interest or opposing interest to the organization. (Institute of Electrical and Electronics Engineers [IEEE], 2020) Taking it a step further subsection 4 where they assert ethical persons should avoid all illegal activity and bribery in their work. (Institute of Electrical and Electronics Engineers [IEEE], 2020) When considering a candidate the ethical question is what are their ethics, do they also conform to the professional ethics outlined in the ACM and IEEE code of ethics and are they a person that can be trusted with a robust but also restricted organization wide access? In review, for protection from external threats there should be organization wide access but to mitigate internal threats the access should adhere to the principle of least privilege and only be given to an ethical and trustworthy candidate.

## References

Association for Computing Machinery. (2018). ACM code of ethics and professional conduct. https://www.acm.org/code-of-ethics

Institute of Electrical and Electronics Engineers. (2020). IEEE code of ethics. https://www.ieee.org/about/corporate/governance/p7-8.html