BTAC BULLETIN

BEHAVIORAL SCIENCE | THREAT ASSESSMENT & MANAGEMENT | LAW ENFORCEMENT & COUNTERINTELLIGENCE | CYBERSECURITY I EMPLOYEE LABOR RELATIONS

PRIVACY & ETHICS

THE DUTY OF INSIDER THREAT PROGRAMS TO LEAD BY EXAMPLE

Insider threat (InT) professionals make decisions daily that have profound impacts on personnel concerning very private issues as well as information protected by civil liberties. Everything from first amendment rights to family upheaval to medical issues are considered when deciding how to mitigate InT risk. As professionals, insider threat personnel have an inherent duty to protect that information which may pass in front of them. They must balance duty and respect to the individual and private information, but also an adherence to an ethos to comply with industry standards and lead by example when handling or discussing highly sensitive information. The U.S. Government (USG) has established 14 general principles of ethical conduct for government employees[1], and every department and agency has ethics officers. But there is no codified set of ethical guidelines particular to the operation of InT programs. This is why it is vital for InT leaders to create a culture of ethics as a starting point while policies and formal training are developed.

GUIDELINES FOR INSIDER THREAT PROFESSIONALS

1 **Maintain professional competency -** The basis of insider threat and risk reduction is a rigorous evidence-based practice. It's important to maintain competency and keep up to date on all the new research and best practices. (Visit ***CDSE*** for updated training.)

2 **Balance timeliness with analysis -** There may be a tendency to rush into decisions given limited evidence and fear of adverse outcomes. It is important to adhere to ethical standards by taking time to collect and analyze the right information, while balancing potential outside pressures and the need ensure timely action.

3 **Strive for a whole-person view of insider threat -** While certain data points, although few in number, may increase concern and impel us toward rapid decision-making out of understandable concern, it is important to not jump to conclusions based on minimal evidence, and to consider both the protective and risk factors in every situation.

4 **Maintain objectivity -** Insider threat professionals deal with sensitive political topics, high visibility individuals, and behavior that may end up in the media. It is vital that professionalism is primary and that personal views do not impact the analytic process. To avoid subjectivity, it is recommended to use structured professional judgment (SPJ) tools and to develop standardized, research-based decision-making rubrics and practices.

DETER
DETECT
MITIGATE
PROTECT
Qui curat protegit

5 **Lead by example when protecting information –** As a gatekeeper of private, confidential, and classified information, InT professionals must have the highest standards in the protection and handling of information. From considerations of unauthorized disclosure to "need to know" to the concerns about weaponizing information, the sanctity of information maintenance is paramount to ensure trust in the system.

6 **Adhere to a standard of nonmaleficence -** While persons of concern may breach societal norms, security standards, and potentially ascribe to ideologies that we do not agree with, it is vital for insider threat professionals to remain objective, avoid ideological judgment or conflict, and focus on behaviors of risk and minimally invasive mitigation strategies to deter, detect, mitigate, and protect highly valuable information and people within the workforce. Doing this through a "do no harm" standard maintains professionalism and trust in the enterprise.

COSTS OF BREACHES OF TRUST/PRIVACY

Potential Consequences to Persons of Concern	*Potential Impact to Organizations*
> Harm to reputation	> Increased InT risk of maladaptive behaviors
> Harm to mental health	> Degradation of team trust/respect
> Loss of productivity	> Loss of productivity
> Loss of work assignment	> InT program loss of trust which could lead to loss of authority, mission, resources, etc.
> Loss of promotion	> Litigation
> Termination	
> Litigation	

1. US Office of Government Ethics (UGOE) 14 General Principles. (Accessed 1/21/25)