Session #1 The Guilty employee

You are the Security Officer for your company. Jimmy shows up in your office often reporting white noise type of incidents: things that are not really security incidents, but they take your time and may result in emails clarifying security policy. Other employees bring you complaints based on intervention from Jimmy, who provides them with incorrect security guidance. In addition to providing the inaccurate guidance, Jimmy occasionally makes his own security mistakes. For example, he left a company laptop in a car that was broken into. Luckily, the car laptop was not stolen, and he was admonished by security and his supervisor, Dena.

What are some insider threat indicators he displays?

a. Access attributes (privileged users, access to proprietary information, leadership, etc.).
b. Professional lifecycle and performance (complaints, substandard work, disgruntled employee, unauthorized absence, etc.).
c. Foreign Considerations (Foreign government interests, foreign assets, receiving benefits from foreign nation).
d. Security and compliance history (security/compliance violations, non-compliance, negligence, misuse of privileges, etc.).
e. Technical activity (violating acceptable user policy, anomalies in data usage or exfiltration, unusual data access request, etc.).
f. Criminal, violent, or abusive behavior (threats to employees or company, criminal activity, sexual assault, or harassment).
g. Substance abuse issues (drinking on the job, Illegal substance use, drug test failure).
h. Financial considerations (debt suddenly is cleared up, unexplained affluence after long periods of debt, financial crimes, etc.).
i. Judgement and Character Issues (falsifying employment information or data, anti-social and compulsive behavior, endorsing workplace violence or abuse, past lack of candor.

How would you deal with an employee like this?

What are some steps you can take to minimize their disruption?

Who may be your partners from the ITP who can help you handle this employee? Please explain your choices

- Legal
- Compliance
- Security
- Human Resources
- C-Suite representatives to include representative of the CTO, CISO, or CIO
- IT Operations
- Security Engineering
- Finance
- Product Management
- Science and Technology
- Business Operations
- Media