COMPANY LOGO

Insider Threat Program Plan for COMPANY NAME.

1. **Purpose**. This plan establishes policy and assigns responsibilities for the Insider Threat Program (ITP). The ITP will seek to establish a secure operating environment for personnel, facilities, information, equipment, networks, or systems from insider threats. An insider threat is defined as ***"the likelihood, risk or potential that an insider will use his or her authorized access, wittingly or unwittingly to do harm to the security of the United States.*** Insider threats may include harm to contractors or program information to the extent that the information impacts the contractor or agency's obligations to protect classified national security information. The program will gather, integrate, and report relevant and credible information covered by the 13 personnel security adjudicative guidelines that may be indicative of a potential or actual insider threat to deter all contractor employees granted personnel clearances (PCLs) and all employees being processed for PCLs, from becoming insider threats; detect any cleared person with authorized access to any government or contractor resources to include personnel, facilities, information, equipment, networks, or systems, who pose a risk to classified information; and mitigate the risk of an insider threat as defined above.

2. **Scope and applicability.** This Insider Threat Program Plan applies to all staff offices, regions, and personnel with access to any government or contractor resources to include personnel, facilities, information, equipment, networks, or systems.

3. **Guiding Principles.**
   a. is subject to insider threats and will take actions to mitigate or eliminate those threats.
   b. will continually identify and assess threats to the organization and its personnel and institute programs to defeat the threats.

4. **Policy.**
   a. The ITP will be established to protect personnel, facilities, and automated systems from insider threats in compliance with 32 CFR 117 of the "National Industrial Security Program (NISPOM Rule). This program will seek to prevent espionage, violent acts against the Nation or the unauthorized disclosure of classified information; deter cleared employees from becoming insider threats; detect employees who pose a risk to classified information systems and classified information; and mitigate the risks to the security of classified information through administrative, investigative, or other responses.

b. The ITP will meet or exceed the minimum standards for such programs, as defined in 32 CFR 117 with additional guidance provided in Industrial Security Letter (ISL) 2016-02 and Defense Security Service (DSS) ODAA Process Manual for Certification and Accreditation of Classified Systems under the NISPOM.

c. The responsibilities outlined below are designed to enable the ITP to gather, integrate, centrally analyze, and respond appropriately to key threat-related information. The ITP will consult with records management, legal counsel, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, and civil liberties issues (including, but not limited to, the use of personally identifiable information) are appropriately addressed.

5. **Responsibilities.**

a. Insider Threat Program Senior Official (ITPSO), will be designated in writing and will act as the company's representative for ITP implementing activities. The designated ITPSO will be cleared in connection with the facility clearance, be a United States citizen, and will be designated as Key Management Personnel (KMP) in NISS in accordance with Cognizant Security Agency (CSA) guidance and in accordance with 32 CFR 117. Upon completion of this memo, (**YOUR ITPSO NAME**) will be appointed at the ITPSO.

b. The ITPSO will be responsible for daily operations, management, and ensuring compliance with the minimum standards derived from DoD Policies. Responsibilities include:

(1) Self-certify the Insider Threat Program Plan in writing to DSS no later than 6 months from the issue date of 32 CFR 117.

(2) Provide copies of the Insider Threat Plan upon request and will make the plan available to the DCSA during the Security Vulnerability Assessments (SVA).

(3) Establish an Insider Threat Program based on the organization's size and operations.

(4) Provide Insider Threat training for Insider Threat Program personnel and awareness for cleared employees.

6. a. Insider Threat Program Management Personnel Curriculum INT312.CU will be used for those who will work within a HUB or working group. Additionally, Insider Threat Annual training will be accomplished via (YOUR TRAINING TOOL OR SYSTEM).

i. A HUB will be created on a ad-hoc basis or when required. The ITPSO will maintain the duties solely until otherwise required.

b. The use of (will be maintained and used annually for cleared employees. First prior to any access to classified information than annually thereafter.

(5) *Establish user activity monitoring on classified information systems in order to detect activity indicative of insider threat behavior. These monitoring activities

will be based on Federal requirements and standards (Federal Information Security Management Act, National Institute of Standards and Technology, and Committee for National Security Systems) and in accordance with ODAA Policy.

a. The use of (EMAIL) weekly download reports or email weekly monitoring reports will be sufficient as a review by the ITPSO.

b. There may be times when the ITPSO will need to contact the email service provider to obtain actual downloaded information. When this occurs, the Senior Manager will be notified due to legal and cost implications.

(6) *Establish procedures in accordance with 32 CFR 117, to access, gather, integrate, and provide for reporting of relevant and credible information across the contractor facility (e.g., human resources, security, information assurance, and legal review) covered by the 13 personnel security adjudicative guidelines that may be indicative of a potential or actual insider threat to deter employees from becoming insider threats; detecting insiders who pose a risk to classified information; and mitigating the risk of an insider threat.

(7) *Establish a system or process to identify patterns of negligence or carelessness in handling classified information, in accordance with 32 CFR 117, even for incidents that do not warrant a culpability or incident report.

(8) *Conduct self-inspections of the Insider Threat Program in accordance with 32 CFR 117.

(9) *Oversee the collection, analysis, and reporting of information across the company to support the identification and assessment of insider threats.

(10) *Establish and manage all implementation and reporting requirements, to include self-assessments and independent assessments, the results of which shall be reported to Senior Management.

6. Insider Threat Incident Investigations

1. Incident Detection
    - Identify suspicious activities through monitoring tools, employee reports, or external notifications.
    - Use behavioral and technical indicators, such as unauthorized data access or unusual workplace conduct, as triggers for further review.
2. Immediate Risk Assessment
    - Determine if the suspected activity poses an immediate threat to critical assets or personnel.
    - Take immediate protective actions, such as revoking access or isolating affected systems, to prevent further damage.
3. Assemble an Investigation Team

- Form a dedicated group with representatives from cybersecurity, HR, legal, and security teams. If necessary, involve external specialists or law enforcement.

4. Evidence Collection
    - Collect relevant data, including logs of network activity, physical access records, and communications (emails, messages).
    - Preserve the integrity of evidence for legal admissibility (e.g., use forensic tools).
5. Conduct Interviews
    - Interview individuals involved in or witnessing the incident.
    - Approach interviews with discretion to avoid tipping off the potential threat actor
6. Analyze Findings
    - Correlate behavioral, technical, and contextual data to understand the scope and intent of the suspected threat.
    - Look for patterns, such as repeated violations or access to sensitive information without a valid business need.
7. Determine and Report Findings
    - Assess whether the activity constitutes a legitimate insider threat.
    - Document findings thoroughly and create a final report detailing the investigation process, results, and recommended actions.
8. Take Corrective Actions
    - If an insider threat is confirmed:
        - Implement disciplinary measures, such as termination or legal action.
        - Mitigate damage by addressing system vulnerabilities or compromised assets.
9. Communication and Notification
    - Notify relevant stakeholders, such as senior management, security officers, and, if required, government agencies (per 32 CFR 117 reporting requirements).
    - Notification to DCSA ISR and CI should be completed at the following stages
        i. Initial Report (what happened)
        ii. Follow up report (what we have learned)
        iii. Final Report (include any incident reports entered into the DoD System of Record)
10. Follow-Up and Lessons Learned
    - Review the incident to identify gaps in policies, training, or monitoring.
    - Update your insider threat program to prevent similar incidents in the future.

ITPSO SIGNATURE BLOCK / COSIGNED BY SMO