**Insider Threat Program Plan**

**December 2016**

**(*Revised August 2023*)**

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 contractor or program information to the extent that the threat impacts the contractor or agency’s obligations to protect classified national security information. The Insider Threat Program will gather, integrate, and report relevant and credible information covered by Security Executive Agent Directive 4 (SEAD 4) – *National 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.

The SEAD 4 – National Security Adjudicative Guidelines are: Allegiance to the United States; Foreign Influence; Foreign Preference; Sexual Behavior; Personal Conduct; Financial Considerations; Alcohol Consumption; Drug Involvement; Psychological Conditions; Criminal Conduct; Handling Protected Information; Outside Activities; and Use of Information Technology Systems. These factors are considered in our customer’s security adjudicative process to make a determination to grant, or continue to grant, access to classified material. An identified risk in any of these areas may indicate the development of an insider threat.

1. **Scope and Applicability.**

This ITP 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.

1. **Guiding Principles.**
2. E-volve Technology Systems, Inc. is subject to insider threats and will take actions to mitigate or eliminate those threats.
3. E-volve Technology Systems, Inc. will continually identify and assess threats to the organization and its personnel and institute programs to defeat the threats.
4. **Policy.**
5. This ITP is established to protect personnel, facilities, and automated systems from insider threats in compliance with *32 CFR Part 117.7 (d)*, National Industrial Security Program Operating Manual (NISPOM), *Insider Threat Program*. The ITP seeks 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 by gathering, integrating, and reporting relevant and available information indicative of a potential or actual insider threat, consistent with E.O. 13587; and mitigate the risks to the security of classified information through administrative, investigative, or other responses.
6. The ITP meets or exceeds the minimum standards for such programs, as defined in the NISPOM with additional guidance provided by Presidential Memorandum “*National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*”, Industrial Security Letters (ISL), and the Defense Counterintelligence and Security Agency (DCSA) Office of the Designated Approving Authority (ODAA) Process Manual for Certification and Accreditation of Classified Systems under the NISPOM.
7. 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.
8. **Responsibilities.**
9. 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 the National Industrial Security System (NISS) in accordance with Cognizant Security Agency (CSA) guidance and in accordance with the NISPOM.
10. The ITPSO will be responsible for daily operations, management, and ensuring compliance with the minimum standards derived from the NISPOM. Responsibilities include:
11. Self-certify the Insider Threat Program Plan in writing to DCSA.
12. Provide copies of the Insider Threat Program Plan upon request and will make the plan available to the DCSA during a Security Review.
13. Establish an Insider Threat Program based on the organization’s size and operations.
14. Provide insider threat training for Insider Threat Program personnel and awareness for cleared employees.
15. E-volve Technology Systems, Inc. has no classified information systems as of the date of this document. Should E-volve Technology Systems, Inc. obtain classified information systems, the ITPSO shall establish user activity monitoring on E-volve Technology Systems, Inc.’s classified information systems 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 the NISPOM. E-volve Technology Systems, Inc. will use standardized classified network banners informing users that their activity on the network is being monitored for authorized purposes and that unlawful or improper use of the computer can result in criminal or administrative actions against them.
16. Establish an Insider Threat Working Group led by the ITPSO and consisting of the Facility Security Officer (FSO), Chief Executive Officer (CEO), Chief Operating Officer (COO), and Human Resources Director. The Working Group will call upon E-volve Technology Systems, Inc.’s outside legal counsel, as necessary. Additional individuals may be added to the Working Group as appropriate. The members of the Working Group will gather, integrate, and report all relevant and credible information across the contractor facility covered by the SEAD 4 – National 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. The Insider Threat Working Group will meet Quarterly, in person or via VTC. Any member of the Working Group may call additional meetings of the working group, as necessary.
17. Establish a process of having all employees report all security incidents and violations to the FSO, regardless of whether the violations are deliberate in nature. The E-volve Technology Systems, Inc. FSO will keep a record of all incidents and violations to include patterns of negligence or carelessness in handling classified information, in accordance with the NISPOM, even for incidents that do not warrant a culpability or incident report. These reports will be reviewed during the Insider Threat Working Group meetings, as appropriate.
18. Review our security program on a continuing basis and will conduct a formal self-inspection at least annually. E-volve Technology Systems, Inc. will use the Center for Development of Security Excellence (CDSE) DCSA Self-Inspection Handbook for National Industrial Security Program (NISP) Contractors as the standard for our DCSA self-inspections to include an insider threat assessment. For other cognizant security agencies, E-volve Technology Systems, Inc. will use the appropriate Self-Inspection guidelines and/or checklists as necessary. Following our self-inspection, E-volve Technology Systems, Inc. will prepare a formal report describing the self-inspection, its findings, and resolution of issues found and retain this formal report for DCSA or other cognizant security agency review through the next Security Review. The E-volve Technology Systems, Inc. CEO will certify to DCSA, and other cognizant security agencies as appropriate, in writing on an annual basis that a self-inspection has been conducted, that senior management has been briefed on the results, that appropriate corrective action has been taken, and that management fully supports the company’s security program.
19. Oversee the collection, analysis, and reporting of information across the company to support the identification and assessment of insider threats. E-volve Technology Systems, Inc. will use automated computer monitoring data, IT audit logs, and facility physical access control records when these are used to protect classified materials in E-volve Technology Systems, Inc.’s possession and when available to E-volve Technology Systems, Inc. E-volve Technology Systems, Inc. will use security files (to include personnel security file information; records of violations, infractions, and incidents; and security clearance information), personnel files containing information about misconduct and adverse actions, travel data, and financial data and disclosure statements to analyze the data for insider threats.
20. Establish and manage all implementation and reporting requirements, to include self-assessments and independent assessments, the results of which shall be reported to the senior management. The E-volve Technology Systems, Inc. ITPSO will manage and implement the ITP to include scheduling the Insider Threat Working Group meetings, submitting all required reports to the CSA, participating in the self-inspections and any other independent assessments.
21. **Insider Threat Training – *32 CFR Part 117.12 (g)*.**
22. ITPSO Training.
23. Initial ITPSO training was completed by 7 December 2016.
24. Whenever a new ITPSO is appointed after the six-month implementation period, the new ITPSO will complete the required training within 30 days of being assigned ITPSO responsibilities.
25. Insider Threat Program Management Personnel Training.
	1. The E-volve Technology Systems, Inc. ITPSO, *and* members of the Insider Threat Working Group (ITWG) will attend the training outlined in the NISPOM and ISLs. These individuals will take the following courses:
* Establishing an Insider Threat Program (*One Time*):
	+ Establishing an Insider Threat Program for Your Organization: [Course INT122.16](https://www.cdse.edu/Training/eLearning/INT122/)
* Insider Threat Awareness (*Annually*): Any in-house training compliant with the NISPOM *or* any CDSE course established by the NISPOM.
	+ Insider Threat Awareness, [Course INT101.16](https://www.cdse.edu/Training/eLearning/INT101/)

or,

* + Counterintelligence Awareness & Security Brief: [Course CI112.16](https://www.cdse.edu/Training/eLearning/CI112/)
	1. After initial implementation of this plan and completion of the required training, all new contractor personnel assigned duties related to the ITP management will complete the above training within 30 days of being assigned duties and refresher training annually thereafter.
1. Employee Insider Threat Awareness Training.
2. E-volve Technology Systems, Inc. required all employees already in access, to complete employee awareness training by 1 May 2017, and annually thereafter in accordance with the NISPOM. Employee awareness training courses may be any in-house training compliant with the NISPOM or any CDSE course established by the NISPOM, such as the two courses listed above {6(b)(1) Insider Threat Awareness}.
3. Moving forward, E-volve Technology Systems, Inc. will require all new hires and/or those cleared employees who are not currently in access to complete employee awareness training before being granted access to classified information and annually thereafter in accordance with the NISPOM. Employee awareness training courses may be any in-house training compliant with the NISPOM or any CDSE course established by the NISPOM, such as the two courses listed above {6(b)(1) Insider Threat Awareness}.
4. Insider Threat Training Records Management.
5. Insider Threat Training Records will consist of training attendance records, certificates, or other documentation verifying those personnel completed the training requirements in accordance with the NISPOM.
6. Insider Threat Program will maintain records of all employee insider threat awareness or program initial and refresher training in accordance with the NISPOM.
7. Insider Threat Training Records will be available for review during DCSA and other CSA Security Reviews.
8. Insider threat awareness will be included in annual refresher training to reinforce, and update cleared employees on the information provided in initial training in accordance with the NISPOM.
9. **Insider Threat Reporting Requirements.**

The Covid-19 Pandemic has affected everyone to some degree and created life changing situations and events for many families, which are still being felt today. These changes have increased the focus on self-reporting requirements and reportable actions by others. All credible insider threat information will be coordinated and shared with the ITPSO using the “*E-volve Technology Systems, Inc. ITP Plan Suspicious Behavior Report Form*” attached. The reporting form will be used by an employee to make a report or to document in person reports or reports taken by phone (i.e., HR representative takes a report from an employee and needs to provide the information to the ITPSO). The ITPSO will then act as directed per SEAD-3, “*Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*.” The following information will be reported:

1. Information regarding cleared employees, to include information indicative of a potential or actual insider threat and which falls into one of the 13 Personnel Security Adjudicative Guidelines, which must be reported when that information constitutes adverse information, in accordance with the NISPOM.
2. Adverse information events that include security violations, security infractions, and workplace violence.
3. Termination of an employee from employment for cause. If that individual was employed on a federal installation, the contractor shall furnish a copy of the report and its final disposition to the Government Contracting Activity (GCA) security Point of Contact (POC) for the respective programs the employee was supporting.
4. Incidents that constitute suspicious contacts, in accordance with the NISPOM (Suspicious Contacts) and ISLs.
5. Information coming to the ITP’s attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations must to be reported to the nearest Federal Bureau of Investigation (FBI), with a copy to the CSA, in accordance with the NISPOM and ISLs.
6. Information determined to be any possible or potential successful penetration of a classified information system must be reported immediately to the CSA per the NISPOM.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Tanya D. Johnson*Insider Threat Program Senior Official* |  | Date Signed |