**INSIDER THREAT SECURITY PROGRAM MANUAL**

**DISCLAIMER OF WARRANTIES**: The content of this manual is not guaranteed to be up to date, and the authors expressly disavow any obligation to update any material that may later be modified, overruled, repealed or superseded by law or regulation. We make no representations or warranties as to the legality or completeness of the material presented herein, and we assume no responsibility for errors that may appear. Your use of this material is at your own risk and we will not be held responsible for any damages or claims that may result from such use. Your sole remedy for your dissatisfaction with the contents or performance of this manual is to cease using the manual. The information contained in this program manual does not represent legal advice and is primarily intended as a public service to the security community in order to provide a sample program for the development of individual company programs.

The Insider Threat Security Program Manual was developed and released as part of a joint effort between *St. Johns Optical Systems, LLC*, *Primal Innovation, LLC,* and *Tesseract Sensors, LLC*. Questions or comments regarding the manual can be sent via e-mail to ITSP@entiaventures.com.



 Entia, LLC, 2016

© 2016 by Entia, LLC Insider Threat Security Program Manual (ITSPM) is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. Entia, LLC permits others to modify and build upon this work for non-commercial purposes. Individuals and organizations may redistribute the original and modified versions, but only under the same or a compatible license. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/4.0/.

Individuals may use any or all parts of the provided document, within the boundaries of the established copyright, but should refer to their own legal counsel prior to implementing or adhering to any information presented herein.



COMPANY, LLC. (“COMPANY”)

INSIDER THREAT SECURITY PROGRAM MANUAL

V.20160726

**Table of Contents**

|  |  |
| --- | --- |
| 1. Purpose………………………………………………………………………...
2. Program Goals…………………………………………………………………
3. Success Criteria……………………………………………………………….
4. Insider Threat Defined…………………………………………………………
5. ITSP Management…………………………………………………………….
6. Key Personnel and Departments……………………………………………….
	1. Senior Company Official………………………………………………….
	2. Facility Security Officer…………………………………………………...
	3. Human Resources Department…………………………………………….
	4. Legal Department………………………………………………………….
	5. Information Technologies Department……………………………………
	6. Managers & Supervisors………………………………………………….
	7. Employees & Company Personnel……………………………………….
7. Deterring Insider Threat……………………………………………………….
8. Training Requirements………………………………………………………...
	1. ITPSO & ITSP Staff………………………………………………………
	2. Managers & Supervisors………………………………………………….
	3. Personnel………………………………………………………………….
9. Risk Categories………………………………………………………………...
	1. Personal Risk Categories………………………………………………….
		1. Money………………………………………………………………....
		2. Ideology……………………………………………………………….
		3. Conscience…………………………………………………………….
		4. Ego…………………………………………………………………….
		5. Nationalism…………………………………………………………....
		6. Sexual Activity……………………………………………………….
		7. Connections…………………………………………………………...
	2. Work Risk Categories…………………………………………………….
		1. Performance…………………………………………………………...
		2. Violations……………………………………………………………...
		3. Security Weakness…………………………………………………….
	3. Targeting Risk Categories…………………………………………………
		1. Foreign Travel………………………………………………………...
		2. Exposure………………………………………………………………
		3. Knowledge & Access…………………………………………………
	4. Insider Threat Risk Tracker (ITRT)………………………………………
		1. ITRT Information…………………………………………………….
		2. Calculating Risk Level……………………………………………….
	5. In Conjunction with Adjudicative Guidelines…………………………….
10. Information Gathering……………………………………………………….
	1. Information Sources……………………………………………………...
		1. Requests for Company Records or Actions………………………….
	2. Privacy……………………………………………………………………
	3. Exception to Privacy…………………………………………………….
	4. Company Sources………………………………………………………...
		1. Facility Security & Counterintelligence…………………………….
		2. Human Resources……………………………………………………
		3. Information Technology & Information Assurance…………………
		4. Company Personnel………………………………………………….
		5. Computer & Workstation Monitoring……………………………….
		6. E-mail Monitoring…………………………………………………...
		7. Telephone Monitoring……………………………………………….
		8. Access Control……………………………………………………….
		9. Mobile Devices………………………………………………………
			1. Company-owned Mobile Devices……………………………….
			2. Bring Your Own Device (BYOD)………………………………
		10. Audio & Video Monitoring………………………………………...
		11. GPS Tracking………………………………………………………
		12. Postal Mail………………………………………………………….
	5. Open Sources…………………………………………………………….
		1. Social Media…………………………………………………………
		2. Civil & Criminal Databases………………………………………….
		3. Other Public Records………………………………………………...
	6. Physical Searches………………………………………………………...
	7. Other 3rd Party Sources………………………………………………….
	8. Legal Considerations…………………………………………………….
	9. Ethical Considerations…………………………………………………...
11. Monitoring Risk………………………………………………………………
	1. Initial Risk Levels……………………………………………………….
	2. Applying Resources……………………………………………………...
		1. Individual Risk Levels……………………………………………….
		2. Targeting Risk Levels……………………………………………….
	3. Updating Risk Levels…………………………………………………….
12. Monitoring Threats…………………………………………………………...
	1. Insider Threat Incident Response………………………………………...
		1. Initial Response……………………………………………………...
		2. Secondary Response…………………………………………………
		3. Formal Inquiry……………………………………………………….
		4. Countermeasure Implementation…………………………………….
13. Reporting Requirements……………………………………………………...
	1. Classified Information……………………………………………………
	2. Cleared Personnel………………………………………………………...
	3. Actual, Probable or Possible Espionage, Sabotage, or Subversion………
14. Quality Assurance…………………………………………………………….

Attachment 1: Risk Categories and Guidelines…………………………………...Attachment 2: ITSP Access/Action Request Form……………………………….Attachment 3: Workplace Search Policy………………………………………….Attachment 4: Monitoring Risk Flowchart……………………………………….Attachment 5: Incident Response Team – Representatives……………………….Attachment 6: ITPSO Appointment Letter………………………………………. | 111222333333334445555666667777778888889101010111111111212121212131313131313131414141414151515161616161617171717171818191919191919202324252627 |

INSIDER THREAT SECURITY PROGRAM MANUAL

1. PURPOSE. The Insider Threat Security Program Manual (ITSPM) provides the structure for the establishment and execution of the Company’s Insider Threat Program, identified as the Insider Threat Security Program (ITSP) in accordance with Executive Order 13587, the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Department of Defense 5220.22-M Incorporating Change 2, and Industrial Security Letter 2016-02. The primary purpose of this program is the detection of actual or potential Insider Threats who pose a risk to classified programs and steps which will be taken to mitigate such risks. The secondary purpose of this program is the detection of actual or potential Insider Threats who pose a risk to Company proprietary information, critical programs, or Information Systems and methods necessary to minimize or mitigate these risks. This program manual will:
* Define “Insider Threat” and identify potential personal, work, and targeting risk areas which may lead to the loss of, or unauthorized access to, U.S. Classified Information or Company proprietary information, critical programs, or Information Systems.
* Provide procedures for gathering relevant information and the processes for accessing, sharing, compiling, and reviewing this information with key personnel and Company departments (e.g. human resources, legal, department heads).
* Identify reporting requirements within the Company and to cognizant security agencies.
* Establish the training requirements for personnel assigned to work in support of the ITSP along with initial, annual, and supplemental Insider Threat training for all personnel subject to the ITSP.
1. PROGRAM GOALS. While the primary goal is preventing the loss of Classified, Proprietary, or Intellectual Property Information (“Information”), it is essential for individuals involved with the ITSP to understand that a major goal of the program is the mitigation of individual risks factors that could lead to Insider Threat actions. A significant portion of the ITSP is the gathering and review of information in order to determine potential risks. However, the intent of this information gathering is not for the purpose of taking direct action against any individual, but to identify personnel who may present a higher risk to the Company. By identifying higher risk personnel, the Company will be better able to both utilize internal resources to reduce potential loss as well as take steps to assist those individuals with methods to reduce their risk or exposure.
2. SUCCESS CRITERIA. Success of the ITSP is difficult to ascertain on a day to day basis due to the numerous variables incorporated into such a program. Success can be narrowly defined as the prevention of any loss of Information, sabotage, or unauthorized access to the Company’s Information Systems due to insider actions. However, actual loss or compromise may be difficult to detect or account for due to the very nature of an Insider Threat. The program’s success can be better defined in a broad view as the deterrence of Insider Threat activity through an active employee training and awareness program, consistent review of potential risk factors, the early identification of personnel exhibiting risk factors, and the utilization of mitigation techniques to reduce those risks.
3. INSIDER THREAT DEFINED. Insider Threats are representative of a danger to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, proprietary information, and computer systems. The insider may perform unauthorized acts against the Company, such as information theft, system compromise, sabotage, corrupting processes, or any other act which would have a negative impact on the Company or its operations.

Insider Threat risks are broken down into two categories which are separated based on the intent of the individual involved.

* **Active**: Those personnel who take deliberate actions against the Company while knowingly violating policies or legal restrictions. This category includes any individual who chooses to take such actions regardless of whether they are doing so for personal reasons (e.g. revenge or financial gain) or if they have been compromised in such a way as to allow a third party to direct their actions (e.g. blackmail or coercion).
* **Passive**: Those personnel who do not have any direct malicious intent. However, their actions or inactions accidentally or inadvertently result in loss or compromise of Information (e.g. opening e-mails with malware attachments or improperly loaning access credentials to a co-worker).
1. ITSP MANAGEMENT. The Company will formally appoint an Insider Threat Program Senior Official (ITPSO) who will be responsible for administering all requirements of the ITSP and ensuring the ITSP is administered in compliance with any applicable laws, regulations, and policies, particularly with respect to workplace rights and privacy. The ITPSO will be cleared in connection with the Company’s Facility Clearance (FCL) and identified as Key Management Personnel within the Electronic Facility Clearance System. The ITPSO must be a U.S. citizen employee of the Company and a senior Company official. The Facility Security Officer may serve as the ITPSO. Attachment 6 contains the standard appointment letter template.

Additional ITSP Team members may be assigned to the ITPSO and will be responsible for such duties as they are appointed. ITSP Team members will be cleared in connection with the Company’s FCL.

1. KEY PERSONNEL AND DEPARTMENTS. The ITSP requires coordination, collaboration, and partnership throughout all levels of the Company in order to be effective. The following list breaks down roles and responsibilities associated with the ITSP. Changes to Company structure, organization, or hierarchy will require a review of the relevant sections and their responsibilities.
	1. Senior Company Official. Appoints the ITPSO, signals their support of the ITSP through written memorandum, and provides senior management support for the implementation and execution of the ITSP.
	2. Facility Security Officer. Coordinates with the ITPSO at all stages of the implementation and execution of the ITSP. Assists with investigations, reports on any actions or activities which could be indicative of Insider Threat activity, and provides information which affects individual risk categories.
	3. Human Resources Department. Provides guidance to the ITPSO regarding relevant changes to labor and employment laws, regulations, and policies which could affect information gathering. Assists with investigations into potential violations or malicious activity. Refers information to the ITSP team that is relevant to risk categories. Works with the ITPSO to develop organizational policies which aid in the reduction of Insider Threat activity.
	4. Legal Department. Provides guidance to the ITPSO regarding legal considerations of the ITSP and assists with investigations into potential violations or malicious activity.
	5. Information Technologies Department. Assists the ITPSO with necessary access to Company systems as needed to conduct authorized investigations. Reports unauthorized access to Company systems along with detected deviations within the systems. Supports the ITSP by monitoring any information system based analytic detection tools. Works with the ITPSO to develop policies, controls, training tools, and safeguards to mitigate the risk of unauthorized access to Information Systems.
	6. Managers & Supervisors. Submit information to the ITPSO that is relevant to risk categories. Reports incidents and violations in regards to Company policies or activities which could be indicative of Insider Threats. Support the ITPSO when conducting investigations into potential Insider Threat activity.
	7. Employees & Company Personnel. Submit information to the ITPSO that is relevant to risk categories. Reports incidents and violations in regards to Company policies or activities which could be indicative of Insider Threats. Note that cleared employees have required reporting obligations established under the National Industrial Security Program.
2. DETERRING INSIDER THREAT. Deterrence is most effective when a comprehensive detection program is in place and employees are encouraged to act as stakeholders in the protection of Company resources. The best way to achieve this goal is to ensure that employees receive sufficient training in order to understand the full scope of how Insider Threats affect the government, the Company, their co-workers, and themselves.

Employees should be made aware of the ITSP and the steps taken by the ITPSO to prevent the risk of Insider Threats. Initial Insider Threat Awareness Briefings will include a basic overview of what steps are taken by the ITPSO to gather information regarding potential employee risks. This should also include an explanation of what safeguards are in place to protect information gathered from improper use. A better understanding of the ITSP can serve as a deterrent against both Active and Passive Insider Threats.

The ITPSO and ITSP Team must also continually work to identify methods and actions which can be used to assist higher risk personnel with ways to reduce, offset, or mitigate those issues that increase the possibility that they could become an Insider Threat, either Active or Passive. At their discretion, the ITPSO may contact any individual who is subject to the ITSP and work with them in order to resolve issues which may be identified as contributing to a personal increase in risk.

1. TRAINING REQUIREMENTS. All training conducted in support of the ITSP will be documented and retained for as long as the individual is associated with the ITSP and for an additional two (2) years after their separation from the program. This includes both ITSP Staff and Company personnel. The ITPSO is responsible for selecting or developing relevant training which meets or exceeds the requirements set forth in DoD 5220.22-M, 3-103. All personnel will be provided initial training prior to being given any insider access. Refresher and sustainment training will be provided on an annual basis. Additional training beyond these minimum requirements will be conducted as directed by the ITPSO in order to maintain effective safeguarding.
	1. ITPSO & ITSP STAFF. There is a significant amount of training and knowledge required to fully implement the ITSP. ITSP Staff must complete initial training within 30 days of being assigned to ITSP duties. Continuous training is also a necessity in order for the ITPSO and ITSP Staff to stay current with, and adapt to, fundamental security changes related to Insider Threat. At a minimum the ITSP personnel must complete training in the follow areas:
* Counterintelligence and security fundamentals, including applicable legal issues;
* Procedures for conducting Insider Threat response actions;
* Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information;
* Applicable laws, regulations, policies, and executive orders along with workplace rights, particularly with respect to free speech and privacy;
* Reviews of Insider Threat case studies.
	1. MANAGERS & SUPERVISORS. Personnel in direct management positions are uniquely situated to assist with the detection of potential Insider Threat risks. As such it is essential that they have an understanding of the ITSP which permits them the ability to identify risk category information or potential threat indicators within their programs or departments. Managers and supervisors will receive training that includes the following areas:
* Guidelines for coordinating with the ITSP Team for Insider Threat investigations;
* The importance of detecting potential Insider Threats by cleared employees and reporting suspected activity to the ITSP Team;
* Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within Information Systems;
* Indicators of Insider Threat behavior, and procedures to report such behavior;
* Applicable counterintelligence and security reporting requirement.
	1. PERSONNEL. All individuals who have insider access to Company Information, including employees, interns, consultants, etc. (“Personnel”), will be provided training in the following areas:
* The importance of detecting potential Insider Threats and reporting suspected activity to the ITSP Team;
* Methodologies of adversaries used to recruit trusted insiders and collect Information, in particular within Information Systems;
* Indicators of Insider Threat behavior, and procedures to report such behavior;
* Applicable counterintelligence and security reporting requirements.
1. RISK CATEGORIES. There are numerous factors that can play a part in the potential for an individual to become an Insider Threat or to be targeted by adversary personnel. It is essential to utilize a standardized format that applies to all Personnel in order to track the various issues which might affect risk factors.

All Personnel will be assigned ratings for an “Individual Risk Level” and a “Targeting Risk Level”. The Individual Risk Level is a compilation of multiple categories which identify issues that could affect the chance that an individual will become an Insider Threat. The Individual Risk Level combines information gathered from both “Personal Risk Categories” and “Work Risk Categories” (these categories are broken out and described in sections 9.1 and 9.2). The Targeting Risk Level covers information which may make an individual a more desirable target for gaining information or access, or increase the possibility that they will come into contact with adversary personnel.

An Insider Threat Risk Tracker (ITRT) database will be maintained by the ITPSO in order to document and track issues which affect individual risk categories and to identify overall Risk Levels. Personal and Work Risk Categories will be assigned a rating between one (1) and (10), negligible risk to very high risk. Targeting Risk Categories will be assigned a rating between one (1) and (5), negligible to very high risk.

* 1. PERSONAL RISK CATEGORIES. These risk areas are directly related to an individual’s activities, beliefs, and actions both inside and outside the workplace. Attachment 1 provides guidelines for rating the various categories on a one (1) to ten (10) scale.
		1. **MONEY**. Issues related to financial problems including debts, foreclosures, forced garnishments, or withholdings due to violations. Also includes instances of extravagant spending or purchases beyond current economic ability which could indicate suspicious financial gains.
		2. **IDEOLOGY**. This category covers political, religious, or personal beliefs. An important note to this category is that there are very few specific ideologies that would automatically make an individual an Insider Threat. The risk this category seeks to identify is when there is a potential for conflict between an individual’s ideology and the actions or activities of the Company. Example: an individual has an extremely strong personal belief that all immigrants should be allowed to cross the border without restriction. The individual is employed by a Company that manufactures seismic detection tools for geophysical research, which does not conflict with that ideology. The Company then receives a government contract to adapt the seismic detection tool for border security. This adapted technology will increase security at the border and restrict immigrants from crossing. This could lead to a direct conflict with the individual’s ideology and presents an increased possibility that they will be motivated to become an Insider Threat, as they may take action to either sabotage the project or reveal weaknesses within the system.
		3. **CONSCIENCE**. This category covers an individual’s ethical or moral concerns regarding Company activities or products, as well as government contracts the Company may support. An important note to this category is that there is no specific conscience issue that would automatically make an individual an Insider Threat. The potential for this risk category to become an issue primarily lies in conflicts between the individual’s moral or ethical code and the actions or activities of the Company. Example: there could be an issue if an individual working for a defense contractor on a UAV’s missile system had a strict ethical issue with the use of unmanned craft in a warzone. This same ethical issue would not be a factor if the individual worked for a Company that developed UAVs for search and rescue operations.
		4. **EGO**. This category applies to individuals whose feelings of self-importance lead to issues of an interpersonal or legal nature. A belief that he or she is superior to other people may result in feelings of unfair treatment if they feel that his or her superiority is not properly recognized. He or she may also feel slighted when others fail to follow their lead or give them the respect that they feel they are due. Additionally, ego may result in a belief that they are above the law or that certain rules should not apply to them. This can be identified by violations of legal restrictions (e.g. constant erratic driving which leads to license suspension, aggressive behavior, or sexual harassment) or failure to adhere to Company policies.
		5. **NATIONALISM**. An individual’s commitment or belief in another country or government may increase the risk that they could take direct actions or be influenced into becoming an Insider Threat, especially when their actions directly benefit that country.
		6. **SEXUAL** **ACTIVITY**. This category relates to an individual’s risk of being manipulated or compromised due to their sexual activity or lifestyle. An important note is that this category does not intrinsically consider the activity itself as a risk, only that such an activity, if it is concealed or if the individual feels it is of an embarrassing nature, may place that individual in a position in which they can be manipulated or compromised by adversary personnel. Example: an individual who privately identifies as LGBTQIA may be subject to coercion if they personally feel that it is necessary to hide their activities from others. An individual who has openly identified themselves as LGBTQIA would not be subject to the same risk.
		7. **CONNECTIONS**. Personal relationships with other individuals can become a concern if those other individuals work for competing companies or have ties to foreign countries. The strength or nature of these interpersonal relationships directly affects the level of influence that could be exerted over Company personnel.
	2. WORK RISK CATEGORIES. These risk areas are directly related to an individual’s activity within the work environment as well as their ability to understand and comply with security procedures, including Insider Threat monitoring. Attachment 1 provides guidelines for rating the various categories on a one (1) to ten (10) scale.
		1. **PERFORMANCE**. Issues which affect an individual’s performance within a Company can be indicative of additional problems or result in situations leading to Insider Threat actions. Inability to complete goals or meet deadlines which leads an individual to believe their employment is at risk can also trigger detrimental behavior. Personnel whose connection with the Company is being terminated are also far more likely to remove Information from the Company or take actions against the Company. Note: all individuals who have been given notice of termination, or have submitted a notice of resignation, will automatically be rated as a ten (10) in this category for the remainder of their time with the Company and will be considered to have a Very High Individual Risk Level.
		2. **VIOLATIONS**. Incidents in which an individual violates Company policies can be viewed as a potential indicator of the individual’s inability to follow guidelines for the protection of Company information and systems. Depending on the nature, a violation could also be an indicator of an individual’s resentment towards the Company or point to additional threat activity. A high number of minor, or a single serious, violation may lead the individual to believe that their relationship with the Company could be subject to termination.
		3. **SECURITY** **WEAKNESS**. An individual’s knowledge of security safeguards, their ability to employ them, and their willingness to follow those safeguards affects this rating. This category is particularly useful for identifying potential Passive Insider Threats. Due to the nature of this category it is possible for the ITSP Team to help improve an individual’s rating. This can be accomplished by conducting additional security exercises or remedial training focused on increasing an individual’s security awareness and ability.
	3. TARGETING RISK CATEGORIES. These risk areas reflect the potential for adversary personnel to make approaches to, or assign resources to, individuals in an attempt to compromise or recruit them. These categories are not direct indicators that the individuals themselves could be compromised or recruited. The primary purpose of identifying Targeting Risks is to allow the ITSP Team the ability to better allocate resources in order to protect and support these individuals, such as by providing specialized travel briefings. Attachment 1 provides guidelines for rating the various categories on a one (1) to five (5) scale.
		1. **FOREIGN** **TRAVEL**. Personnel who routinely travel are far more likely to become targets of adversary personnel or be exposed to foreign intelligence gathering organizations. This travel can be for either personal or business reasons. Travel to certain high risk countries can also increase the potential targeting risk.
		2. **EXPOSURE**. An individual’s connection to a classified or proprietary program may lead to an increased chance of targeting. Such exposure could result from an individual posting information on a social media site, a press release from the Company, or even the inadvertent release of Company information.
		3. **KNOWLEDGE** **& ACCESS**. Individuals with high level technical capabilities or sensitive Company Information, including subject matter experts and senior engineers, are at a higher risk of targeting. Additionally, personnel with access to restricted locations or Information Systems, such as Information Technology Administrators, may be targeted as their individual access could provide significant ingress to multiple areas.
	4. INSIDER THREAT RISK TRACKER (ITRT). In order to identify varying levels of risk within the Company, it is necessary to compile the risk categories into a format that allows for consistent tracking. The method established for this is the use of a database entry system that will contain basic information on all Personnel subject to the ITSP, individual ratings for all categories, information relating to the selection of those ratings, and a calculated Individual Risk Level and Targeting Risk Level.
		1. ITRT INFORMATION. Information gathered and compiled as part of the ITSP may be personally sensitive in nature, even when obtained from open source locations. Access to the ITRT will be restricted to the ITSP Team. Release of any information contained within the ITRT, including individual category ratings or risk levels, must be authorized by the ITPSO.
		2. CALCULATING RISK LEVEL. Risk levels are calculated by assigning weighted scores to each Risk Category and then adding those scores together. The resulting total is compared to a pre-determined range in order to identify the Individual and Targeting Risk Levels. Initial weighted scores have been established based on historical modeling (fig.1). The weighted scores and ranges may be modified by the ITPSO if the current scoring model is not properly representative of the Company’s Insider Threat tracking requirements.

Example: An individual receives the following risk levels in four separate categories: Money (3), Ideology (4), Conscience (2), and Ego (6). The weighted scores for each category are 70, 130, 30, and 400. This results in a total of 630. The total calculated score fits within the Medium Calculated Range (521-1599). This would result in an Individual Risk Level of ‘Medium’.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Individual Risk Categories |  | Targeting Risk Categories |  | Calculated Risk Range |
| Rating | Level | Weighted |  | Rating | Level | Weighted |  | Rating | Calculated Range |
| Low | 1 | 0 |  | Low | 1 | 0 |  | Negligible | 0 | - | 150 |
| 2 | 30 |  | 2 | 150 |  | Low | 151 | - | 520 |
| 3 | 70 |  | Medium | 3 | 750 |  | Medium | 521 | - | 1599 |
| 4 | 130 |  | High | 4 | 2000 |  | High | 1600 | - | 4499 |
| Medium | 5 | 250 |  | 5 | 4500 |  | Very High | 4500 | - | ∞ |
| 6 | 400 |  |  |  |  |  |  |  |  |  |
| High | 7 | 700 |  |  |  |  |  |  |  |  |  |
| 8 | 1600 |  |  |  |  |  |  |  |  |  |
| 9 | 3000 |  |  |  |  |  |  |  |  |  |
| 10 | 4500 |  |  |  |  |  |  |  |  |  |

Fig.1 - Baseline Risk Levels and Calculated Risk Range

* 1. IN CONJUNCTION WITH ADJUDICATIVE GUIDELINES. In conjunction with DoD 5220.22-M and ISL 2016-02, the ITSP must have procedures in place for cleared personnel in order to identify and report relevant information covered by the thirteen (13) personnel security adjudicative guidelines that may be indicative of a potential or actual Insider Threat.

The Personal and Work Risk Categories associated with the ITSP can be utilized to identify issues which correspond with specific adjudicative guidelines. These corresponding areas (fig.2) ensure that the ITSP Team can effectively notify the cognizant organization regarding indicators of potential or actual Insider Threat by cross-referencing the specific category and guideline. Note that this is only a guide and certain activities may span multiple categories or affect adjudicative guidelines outside the listed guide.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Personal Risk Categories** | **Work Risk Categories** |
| **Adjudicative Guidelines** | Money | Ideology | Conscience | Ego | Nationalism | SexualActivity | Connections | Performance | Violations | SecurityWeakness |
| A | Allegiance to theUnites States |  | ● | ● |  | ● |  | ● |  |  |  |
| B | Foreign Influence | ● | ● | ● |  | ● | ● | ● |  |  |  |
| C | Foreign Preference |  | ● | ● |  | ● |  | ● |  |  |  |
| D | Sexual Behavior |  |  |  |  |  | ● |  |  |  |  |
| E | Personal Conduct |  |  |  | ● |  | ● |  |  | ● |  |
| F | FinancialConsiderations | ● |  |  |  |  |  |  |  |  |  |
| G | AlcoholConsumption |  |  |  | ● |  |  |  | ● | ● |  |
| H | Drug Involvement |  |  |  | ● |  |  |  |  | ● |  |
| I | PsychologicalConditions |  |  |  | ● |  |  |  | ● | ● |  |
| J | Criminal Conduct |  |  |  | ● |  |  |  |  | ● |  |
| K | Handling ProtectedInformation |  |  |  |  |  |  |  |  | ● | ● |
| L | Outside Activities |  |  |  |  | ● |  | ● | ● | ● |  |
| M | Use of InformationTechnology Systems |  |  |  |  |  |  |  |  | ● | ● |

Fig.2 - Adjudicative Guidelines Cross-Reference Guide

1. INFORMATION GATHERING. An essential component of the ITSP is the ability to collect, compile, and evaluate information pertaining to Company Personnel in order to identify risk factors that could lead to Insider Threat actions or to identify actual Active Insider Threats.

This information may come from a variety of sources and requires the focus of the entire ITSP Team to properly coordinate its collection and review. Information gathered throughout the process may also fall under a variety of legal or ethical restrictions which will impact how the ITSP Team may utilize such information.

* 1. INFORMATION SOURCES. The ITSP Team should be able to utilize any legally obtained source of information when compiling data on potential Insider Threats. However, the primary sources from which information will be collected can be broken down into five (5) areas. These sources are the Company’s Human Resources Department, Information Technology Department, Managers & Supervisors, Co-workers, and Open Sources.
		1. REQUESTS FOR COMPANY RECORDS OR ACTIONS. Requests submitted to any Company department, for information or actions in support of the ITSP, will be documented through a formal request process. A standardized form (Attachment 2) will be utilized. Completed copies of each request will be maintained by the ITSP Team and the servicing department.

These primary sources of information can be cross-referenced with the risk categories to identify those sources most likely to reveal certain types of information (fig.3). It is important to note that relevant information for any category could be gleaned from any source. This reference tool is simply a guide which can be used when attempting to research additional information relating to a particular risk category.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Human Resources | Information Technology | Managers/Supervisors | Co-workers | Open Source |
| Money | ● | ● |  | ● | ● |
| Ideology |  | ● | ● | ● | ● |
| Conscience |  | ● | ● | ● | ● |
| Ego | ● | ● | ● | ● | ● |
| Nationalism |  | ● | ● | ● | ● |
| Sexual Activity |  | ● | ● | ● | ● |
| Connections |  | ● |  | ● | ● |
| Performance | ● | ● | ● | ● |  |
| Violations | ● | ● | ● |  |  |
| Security Weakness |  | ● | ● | ● | ● |
| Foreign Travel | ● | ● | ● | ● | ● |
| Exposure |  |  |  |  | ● |
| Knowledge & Access | ● | ● | ● | ● | ● |

Fig.3 - Information Sourcing Reference

* 1. PRIVACY. All Company Personnel have some expectation of privacy. However, the extent of this privacy differs depending on a number of factors such as the individual’s use of Company-owned technology. Company personnel should have no expectation of privacy in connection with data stored or transmitted via computers, e-mail accounts, phones, or mobile devices that are owned by the Company. Items and work areas belonging to the Company are typically open to search by the Company at any time. As part of the ITSP, a Workplace Search Policy (Attachment 3) will be provided to all Company Personnel advising them of the guidelines and search limitations that the Company has approved for use.

Regardless of the source or reason for collecting information, it must be understood by the ITSP Team that the program is likely to collect information that might be sensitive or embarrassing to individuals, regardless of whether or not the information is obtained from a publicly available and open source. Information regarding an individual’s affiliations, ideologies, or activities which may, or may not be, of direct use in establishing risk levels must be safeguarded from inadvertent release.

At all times the ITSP Team will act in a careful and diligent manner to ensure that information obtained by the ITSP is used solely for the purpose of identifying potential Insider Threats. At no time will information gathered under the ITSP be released to any other individual for purposes outside the scope of the ITSP. This includes, but is not limited to, use of information for determining promotions, demotions, assignments, or any other action which would be for the benefit or detriment of any Company personnel. The ITSP Team will take steps to secure such information through the use of password protected systems, encryption, or any such method that would reasonably be considered sufficient for the protection of personal data.

* 1. IMMEDIATE ACTION EXCEPTION. The ITSP Team will take immediate action should information be gathered that would reasonably be indicative of a threat of physical violence or serious criminal activity, regardless of where the information has been gathered from. These actions can include the notification of law enforcement, conducting no-notice searches, restricting access, or any other action deemed necessary to protect the welfare of Company personnel, visitors, customers, or any other individuals. These actions will be taken regardless of whether they would reveal private or confidential information gained through the ITSP.
	2. COMPANY SOURCES.
		1. Facility Security & Counterintelligence. Facility Security and Counterintelligence Offices will provide access to all relevant databases and files to include, but not limited to, personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings. These offices will also report any information gathered, which is relevant to the ITSP, to the ITSP Team.
		2. Human Resources. The Human Resources Department will provide access to relevant HR databases and files to include, but not limited to, personnel files, payroll and voucher files, outside work and activities requests, disciplinary files, and personal contact records, as may be necessary for resolving or clarifying Insider Threat matters. HR will also report any information gathered which is relevant to individual risk categories, to the ITSP Team.
		3. Information Technology & Information Assurance. Company departments that maintain relevant unclassified and classified networks will provide the ITSP Team with information generated by such elements to include, but not limited to, personnel usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an Insider Threat concern. These departments will also report any information gathered, which is relevant to the ITSP, to the ITSP Team.
		4. Company Personnel. Individuals within the Company are often the best positioned to detect potential indicators of Insider Threat activity as well as changes that would affect individual risk categories. ITSP Team members will take note of both validated information and rumors which might be provided by Company Personnel. Unsubstantiated rumors will be annotated, however, they will not be used to effect any risk category changes unless reasonable supporting evidence can be identified.

Company personnel may request confidential meetings with the ITSP Team. Anonymous notifications may also be submitted to the ITSP Team through a Company e-mail account designated for such notifications. Company personnel will receive training on the options for communicating with ITSP Team and notices will be posted in public areas of the Company containing this contact information.

* + 1. Computer & Workstation Monitoring. The ITSP Team may coordinate with the Information Technologies Department in order to track personnel use of, and access to, Company computers and workstations. This will typically consist of, but is not limited to, the following types of monitoring:
* Utilizing computer software that enables the ITSP Team the ability to see what is on the screen or stored in the individual’s computer terminal and hard disks.
* Monitoring internet usage to include e-mails and websites the user visits.
* Tracking the amount of time individuals spend away from their computer or periods for which the system is idle.
* Monitoring the number of keystrokes per hour in order to determine activity levels.
	+ 1. E-mail Monitoring. The monitoring of Company-owned electronic mail systems may be utilized as necessary to assist with the detection of unauthorized activities. Review of this source can be conducted at more than one level. At the most basic level, the use of analytic software or mail server rules can be used to identify variations in communications. When necessary, reviews can be made of the e-mail addresses that the individual communicates with. The final level of review is direct access to the individual’s e-mail which would allow the ITSP Team to review the full contents and attachments of all messages.

Note: Full access to the contents and attachments of messages will be coordinated with the Human Resources and Legal Departments.

* + 1. Telephone Monitoring. This form of monitoring is strictly controlled and is typically limited to quality control uses. The ITPSO will coordinate with the Legal Department prior to conducting any such monitoring.
		2. Access Control. The ITSP Team may review any building access control records, visitor logs, or other systems which control or monitor entry into any Company-owned or leased facility.
		3. Mobile Devices. The constant use of mobile devices for all aspects of business and personal life represent a substantial source for information regarding employee activities. Monitoring and recording such devices may reveal movements, contacts, risk factors, and potential unauthorized activities.
			1. Company-owned Mobile Devices. Monitoring of Company-owned mobile devices is authorized. The ITPSO will coordinate with the Information Technologies Department in order to initiate any monitoring actions. Such monitoring may include reviews of text messages, email, Web usage, location, contacts, call logs, photos and videos.
			2. Bring Your Own Device (BYOD). The ITPSO will coordinate with the Human Resources and Information Technologies Department prior to conducting monitoring of any BYOD mobile device and must ensure that such monitoring is consistent with the current version of the Company’s BYOD policy and any applicable laws and regulations.
		4. Audio & Video Monitoring. The installation and use of any video monitoring system on Company-owned or leased property must be approved by the Senior Company Official. At no time will video monitoring systems be installed where they are physically invasive (e.g. bathrooms or locker rooms).

Audio recordings will not be made and no audio monitoring may take place unless all involved parties have provided consent. This may occur during investigations or interviews.

* + 1. GPS Tracking. The tracking of Company-owned vehicles through the use of GPS devices is authorized. Note that no tracking will be conducted on vehicles that are privately owned by Company personnel or on any vehicles that are owned by the Company but are approved as a ‘take-home’ vehicle for a Company employee (i.e. a vehicle the Company owns or leases and which the employee is authorized to use for personal travel).
		2. Postal Mail. Mail received at a Company-owned or leased location and addressed to personnel working for the Company may be opened and reviewed. The ITPSO will coordinate with the Legal Department prior to taking such actions to ensure compliance with all applicable laws.
	1. OPEN SOURCES. The availability of open source information will vary depending on each individual’s activities. Some individuals may consistently post updates, upload images, and add comments on a variety of sites. Other individuals may have a minimal on-line presence. It may also be possible to identify risk issues based on the on-line comments of an individual’s friends, family, acquaintances, or co-workers.

Company personnel can become more exposed to targeting based on on-line postings, which are assumed to be anonymous, if it is possible for adversary personnel to connect screen names and digital identities with actual individuals. The ITSP Team will work to identify any such connections in order to identify potential issues. This will generally be completed by identifying and cataloguing individuals’ screen names, personal e-mail addresses, and the consistency with which they utilize these pseudonyms.

* + 1. Social Media. Reviews of social media posts, as well as postings on any forum or on-line chat section, can provide a large amount of insight on possible risk issues. Second and third party postings may also be reviewed.

Note: At no time will any member of the ITSP Team create a false identity for the purpose of gaining access to any individual’s social media account. No Company personnel will be required to provide the ITSP Team with their personal social media logon credentials, nor will any Company personnel be directed to ‘friend’ a member of the ITSP Team or otherwise have access to their social media account forced. It is acceptable for the ITSP Team member to use a personal or Company login or account in order to access the primary site on which the subject individual’s social media account resides. However, only information that is openly available to the public may be reviewed.

* + 1. Civil & Criminal Databases. A large amount of data is publicly available through County Clerk records. Reviews should be made of these databases to determine if an individual has been involved in unreported criminal activity. This source can be used to identify risk issues in multiple categories.

The ITSP Team should identify areas in which each individual lives, works, and commutes through in order to select the most useful databases to review.

* + 1. Other Public Records. Additional public records exist which may be of selective use. These sources include information pertaining to property records, personal legal changes, motor vehicle identification, motor vehicle operator records, etc. Such records may be accessed as needed to identify risk issues.
	1. PHYSICAL SEARCHES. The ITPSO may conduct physical searches authorized by, and consistent with, Company policy (see Attachment 3), along with all applicable laws and regulations. Prior to completing any searches, the ITPSO will coordinate with the Human Resources and Legal Departments. Searches relating to management level personnel (e.g. Program managers and Senior Engineers) must also be approved by the Senior Company Official. Additional technical personnel may be retained by the ITPSO to assist with the search (e.g. to perform forensic work on a laptop).
	2. OTHER 3RD PARTY SOURCES. The ITPSO will determine on a case-by-case basis whether the use of any other source will be in keeping with the goals of the ITSP, as well as being consistent with the legal and ethical considerations established for the program.
	3. LEGAL CONSIDERATIONS. The ITPSO is ultimately responsible for ensuring that the ITSP does not violate any legal guidelines. As such, the ITPSO will review all ITSP activities on a consistent basis and validate the legitimacy of those activities against local, state, and federal laws and regulations. Any activity which violates such laws will be removed from the program or modified so as to comply with the relevant legal guidelines. Note that this manual does not constitute legal advice and the ITPSO will coordinate with the Company’s legal counsel to verify compliance with all relevant statutes and regulations.

A basic framework has been established to guide ITSP Team members in order to assist with maintaining basic legal compliance:

* No information gained through the ITSP will be used to take action against any individual on the basis alone of that individual’s conduct during non-working hours away from the Company's premises or on the basis of personal characteristics unless that conduct or characteristic affects the individual’s ability to properly fulfill the responsibilities of his or her position with the Company (e.g. individual’s ideology conflicts with employment activities).
* The ITSP Team will not attempt to intercept or monitor any legally protected communication sent or received by any individual. Such protected communications include messages or conversations between an individual and their doctor, attorney, or any other legally protected program. Information of this nature that is inadvertently obtained by the ITSP Team will be immediately purged from any ITSP records.
* Comments or activities regarding concerted activities and union activities are protected actions and will not be used when determining risk levels, except when such comments or activities outside the scope of the protections set forth by the National Labor Relations Act.These protected comments or activities include, but are not necessarily limited to, forming a union, attempting to form a union, assisting a union in organizing fellow employees, whenever two or more employees address the Company regarding pay improvements, or when employees discuss work-related issues such as safety concerns and steps to improve workplace conditions.
	1. ETHICAL CONSIDERATIONS. The goal of the ITSP is not to spy on Company personnel or to create a “big brother” environment which would inhibit any individual’s personal activities or lifestyles. All possible effort will be taken by the ITSP Team to ensure that the data being reviewed, collected, and assessed will be directly relevant to the actual reduction or detection of Insider Threat activity.

The ITSP will not directly search for comments or activities that are representative of whistleblower activities. Any information of this type that is received will not be released to individuals that are indicated as being part of the whistleblower’s complaint, unless absolutely necessary in order to validate an Active Insider Threat risk.

1. MONITORING RISK. Each individual subject to the ITSP enters a continuous loop wherein they are monitored for Insider Threat activities as well as any changes to risk categories that could affect the possibility that they may become involved in such activities. By assigning Individual and Targeting Risk Levels, the ITSP Team can then prioritize resources in order to prevent Insider Threat activities. Attachment 4 provides a flowchart of the continuous loop process.

An individual whose relationship with the Company is terminated is still considered to be a potential Insider Threat due to their established knowledge of the Company’s internal procedures and safeguards, proprietary or confidential information which may have been retained prior to their separation, or ongoing grievances by the individual against the Company. For these reasons the ITSP Team will continue to monitor separated Company personnel for at least six (6) months from the time that they officially separate from the Company. Select cases for additional periods of monitoring beyond the six (6) months must be reviewed and approved by the ITPSO.

* 1. INITIAL RISK LEVELS. Once an individual becomes subject to the ITSP, the ITSP Team will conduct an initial assessment for each risk category. Information will be gathered on the individual in order to populate the ITRT with information relevant to the assessment process. Initial Individual and Targeting Risk Levels will be determined in order to assign resources to monitor or assist the individual in order to mitigate the risk of Insider Threat.
	2. APPLYING RESOURCES. There is a limited number of resources allocated to the ITSP. Proper allocation of available resources to the highest levels of risk is the most effective method for countering Insider Threats.
		1. Individual Risk Levels. Resources used to track and detect potential Insider Threat activities consists of ITSP Team time utilized for researching and tracking changes to individual risk categories or conducting assessments on activities or incidents, Insider Threat awareness training, analytic detection tools, support from other Company departments, use of 3rd party investigative and tracking tools, or any other asset that may be utilized in order to identify potential or actual Insider Threats.
		2. Targeting Risk Levels. Resources applied to individuals with higher Targeting Risk ratings consists of ITSP Team time utilized for training of higher risk personnel and providing additional levels and types of protection for those individuals.
	3. UPDATING RISK LEVELS. It may become necessary to raise or lower levels as individual risk categories are assessed or if an Insider Threat situation occurs. Changes to risk category levels will be recorded in the ITRT along with explanations for the level change.
1. MONITORING THREATS. The calculated risk levels serve as a guide for the ITSP Team as to the most useful application of resources (fig.4). Note that this is only a guide and does not restrict the ITSP Team from reallocating or assigning resources as needed.

|  |  |
| --- | --- |
| Risk Level | Description |
| Negligible | No specialized monitoring required unless specific conditions require it. |
| Low | Low level monitoring of activities when resources are available. |
| Medium | Increased monitoring of activities when resources are available. |
| High | Priority focus of resources for continuous monitoring. |
| Very High | Set as primary focus of resources to closely monitor activities. |

Fig. 4 – Resource Prioritization Guide

* 1. INSIDER THREAT INCIDENT RESPONSE. As soon as there is an indication of an actual Insider Threat, the ITPSO will coordinate an Incident Response Team consisting, at a minimum, of representatives from the Human Resources, Legal, Facility Security, and Information Technologies Departments. Additional personnel and departments will be included as needed, based on a determination by the ITPSO. Attachment 5 contains a list of the primary representatives and their contact information. The response to the threat will include four (4) phases: Initial Response, Secondary Response, Formal Inquiry, and Countermeasure Implementation.
		1. INITIAL RESPONSE. The first part of the incident response is focused on stopping a potential threat from materializing or preventing further damage from an incident that has already occurred.

The scope of the response will be based on the type of incident or threat. The first goal of the Incident Response Team is to gather, at a minimum, the following pertinent information:

* Determination if Insider Threat is Active or Passive.
* Identify what information or resources are affected.
* Identify what notifications are required (internal and external).
* If responding to potential threat: What steps can be taken to prevent the threat.
* If an incident has occurred: What steps can be taken to prevent further loss or damage.

Based on this information, the Incident Response Team will designate a course of action and identify required notifications. The ITPSO will implement the plan and make notifications as necessary.

* + 1. SECONDARY RESPONSE. This part of the response is fluid and actions to be taken will be determined by the ITPSO and Incident Response Team based on the exact nature of the incident. The goal of this stage is the complete review of the incident in order to identify the extent of damage, how the damage was done, and responsibility for the incident. Multiple actions and notifications may be required based on the type of incident, information involved, and extent of damage(s).

A primary purpose of this stage is the Company’s coordination with outside agencies as required by law or regulation (e.g. local law enforcement, the Federal Bureau of Investigation, or the Defense Security Service), or with 3rd party specialists retained by the Company for additional investigations and forensics. The ITPSO will typically serve as the Company’s central point of contact throughout the Secondary Response stage.

* + 1. FORMAL INQUIRY. Upon completion of the Secondary Response, the ITPSO will work with the Incident Response Team and cognizant outside agencies to prepare formal documentation regarding the incident. Individual interviews may be conducted by the ITSP Team to gather necessary information or to further assess additional risks associated with the incident.

At a minimum, the report will include the following information:

* When did the incident occur?
* How was the incident identified?
* Type of Insider Threat: Active or Passive?
* Who was responsible for the incident?
* What was the nature of the incident: Theft/Loss, Sabotage, Compromise, Fraud, other?
	+ For Theft/Loss: What Information or property was affected and was it potentially or actually compromised?
	+ For Sabotage: What technologies, Information, equipment, or personnel were affected and what is the extent of the damage?
	+ For Compromise: What systems were affected and how was compromise conducted?
	+ For Other: What was the full extent of the incident and how did it occur?
* List of personnel, departments, and external organizations that were notified.
* Were countermeasures in place to prevent the incident? What type? Did they fail?
* What countermeasures can be implemented to prevent a similar incident?

Additional information pertinent to the incident will be included in the report. The completed final report will be submitted to the Senior Company Official.

* + 1. COUNTERMEASURE IMPLEMENTATION. The ITPSO will work with applicable Company departments and personnel to implement countermeasures identified in the Formal Inquiry.
1. REPORTING REQUIREMENTS.
	1. Classified Information. Any incident which impacts U.S. Government classified information or systems will be reported to the Defense Security Service through the assigned Industrial Security Representative.
	2. Cleared Personnel. Information relevant to the 13 personnel security adjudicative guidelines, that may be indicative of a potential or actual Insider Threat, will be reported to the Defense Security Service for all individuals who have received a U.S. Government Personnel Clearance.
	3. Actual, Probable or Possible Espionage, Sabotage, or Subversion affecting a Cleared Facility. Incidents of this nature will be reported to the Federal Bureau of Investigation and the Defense Security Service.
2. QUALITY ASSURANCE. The Senior Company Official may direct any Senior Management Official to conduct quality assurance reviews or investigations into any alleged misconduct or mismanagement of the ITSP.

ATTACHMENT 1: RISK CATEGORIES AND GUIDELINES

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Money** | 1 | No issues identified or any issues are effectively mitigated. |
| 2 | Minimal issues, concerns, or more serious issues are partially mitigated. |
| 3 |
| 4 |
| 5 | Some issues or concerns affecting financial stability. |
| 6 |
| 7 | Serious issues in excess of current economic standings. |
| 8 |
| 9 |
| 10 | Extreme issues such as foreclosures or unfavorable judgments or extravagant activities far beyond current economic standing. |

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Ideology** | 1 | No issues identified or any issues are effectively mitigated. |
| 2 | Individual expresses some interest in certain political, religious, or personal beliefs. |
| 3 |
| 4 |
| 5 | Individual has strong political, religious, or personal beliefs. The force behind these beliefs is commensurate with, or slightly above, current societal standards. |
| 6 |
| 7 | Individual has very strong political, religious, or personal beliefs and has expressed that these beliefs are above other societal restrictions. |
| 8 |
| 9 |
| 10 | Has extreme political, religious, or personal beliefs above societal restrictions and actively works to promote or carry out these beliefs. |

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Conscience** | 1 | No issues identified or any issues are effectively mitigated. |
| 2 | Has minor ethical or moral concerns regarding Company activities or products. Alternatively, if working on US contracts, the individual has minor ethical or moral concerns regarding US policies or activities. |
| 3 |
| 4 |
| 5 | Has some ethical or moral concerns regarding Company activities or products. Alternatively, if working on US contracts, the individual has some ethical or moral concerns regarding US policies or activities. |
| 6 |
| 7 | Expresses strong ethical or moral concerns regarding Company activities or products. Alternatively, if working on US contracts, the individual expresses strong ethical or moral concerns regarding US policies or activities. |
| 8 |
| 9 |
| 10 | Consistently makes extreme statements regarding ethical or moral issues regarding Company activities, products, or support for US Government.  |

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Ego** | 1 | No issues identified or any issues are effectively mitigated. |
| 2 | Minimal issues, or more serious issues are partially mitigated. |
| 3 |
| 4 |
| 5 | Individual has an above average feeling of self-importance and may easily feel slighted under normal circumstances. Individual believes that they should be exempt from some rules or laws. |
| 6 |
| 7 | Individual feels that they lack importance, feels that they have been treated unfairly, or feels that they have been wronged (either real or imagined). Individual believes that their superiority places them above societal rules or laws. |
| 8 |
| 9 |
| 10 | Expresses or displays a belief that they are superior to others and that their importance is not properly recognized. Rules and laws do not apply to them. |

ATTACHMENT 1 (continued): RISK CATEGORIES AND GUIDELINES

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Nationalism** | 1 | No issues identified or any issues are effectively mitigated. |
| 2 | Has ties to a foreign country due to dual-citizenship, family relations, or presents some other personal connection to a foreign country. |
| 3 |
| 4 |
| 5 | Expresses feelings of connection with a foreign country or government equal to, or above that, of the United States. |
| 6 |
| 7 | Has made verbal, written, or implied statements identifying a desire to aid a foreign country or government. |
| 8 |
| 9 |
| 10 | Expresses great regard for foreign country or government and demonstrates a strong desire or intent to provide them aid without regard for policies. |

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Sexual Activity** | 1 | No issues identified or any issues are effectively mitigated. |
| 2 | Minor issues due to natural age or maturity, or more serious issues are partially mitigated. |
| 3 |
| 4 |
| 5 | Potential for manipulation or coercion due to personal proclivities for non-traditional activities, or hidden lifestyle. |
| 6 |
| 7 | High risk due to hidden lifestyle or potential for manipulation or coercion. Involved with illegal sexual activities such as prostitution (note that involvement may not necessarily include direct participation). |
| 8 |
| 9 |
| 10 | Very high risk of being manipulated or coerced due to sexual activities or behavior. Routinely engages in illegal sexual activities. |

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Connections** | 1 | No issues identified or any issues are effectively mitigated. |
| 2 | Has connections to individual(s) working at competing companies or with foreign ties. |
| 3 |
| 4 |
| 5 | Has personal connections with individual(s) working at competing companies or with foreign ties. These connections exceed basic friendship and may be associated with shared history, goals, or needs. |
| 6 |
| 7 | Has very strong connections with individual(s) working at competing companies or with foreign ties. These connections may be deeply emotional in nature or associated with a long term relationship. |
| 8 |
| 9 |
| 10 | Has extreme bonds of obligation or connections to individual(s) working at competing companies or with foreign ties. |

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Performance** | 1 | No issues identified or any issues are effectively mitigated. |
| 2 | Minimal issues, concerns, or more serious issues are partially mitigated. |
| 3 |
| 4 |
| 5 | Some issues or concerns. |
| 6 |
| 7 | Above average issues that have the potential to result in termination. |
| 8 |
| 9 |
| 10 | Serious performance issues which could result in termination or individual has submitted resignation or has been scheduled for termination. |

ATTACHMENT 1 (continued): RISK CATEGORIES AND GUIDELINES

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Violations** | 1 | No issues identified or any issues are effectively mitigated. |
| 2 | Minimal issues, concerns, or more serious issues are partially mitigated. |
| 3 |
| 4 |
| 5 | Some issues or concerns. |
| 6 |
| 7 | Above average issues that have the potential to result in termination. |
| 8 |
| 9 |
| 10 | Serious violations which could result in immediate termination. |

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Security Weakness** | 1 | Has a thorough understanding of current security risks and consistently takes additional steps to utilizes specialized safeguards. |
| 2 | Has an average understanding of security risks and regularly follows established security safeguards. |
| 3 |
| 4 |
| 5 | Has a basic knowledge of security and typically follows established safeguards. |
| 6 |
| 7 | Has a very rudimentary knowledge of security or consistently fails to follow security safeguards. |
| 8 |
| 9 |
| 10 | Has non-existent knowledge of security risks or deliberately ignores security safeguards. |

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Foreign Travel** | 1 | Individual does not travel outside of local area. |
| 2 | Individual rarely travels outside the local area or the country. |
| 3 | Individual occasionally travels outside the country for work or tourism. |
| 4 | Individual's position requires frequent overseas travel or they routinely travel outside the country for tourism or personal reasons. |
| 5 | Individual makes constant overseas trips with multiple return trips to the same locations/regions or travels to high risk regions. |

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Exposure** | 1 | No connection has been identified linking individual to classified or proprietary projects. |
| 2 | There is only insubstantial info which potentially links individual to classified or proprietary projects. |
| 3 | There is circumstantial data which could link the individual to classified or proprietary projects. |
| 4 | Reference to individual’s work on classified or proprietary projects can be obtained through conversation and/or web based sites. |
| 5 | Individual’s connection to classified or proprietary projects can be easily established through conversation and/or web based sites. |

|  |  |  |
| --- | --- | --- |
| Category | Level | Guidelines |
| **Knowledge & Access** | 1 | No technical knowledge, abilities, or access to proprietary or controlled information. |
| 2 | Minor technical knowledge, abilities, or low level access to systems containing proprietary or controlled information. |
| 3 | Average technical knowledge, abilities, or moderate access to systems containing proprietary or controlled information. |
| 4 | Above average technical knowledge, abilities, or high level access to systems containing proprietary or controlled information. |
| 5 | Subject Matter Expert for classified or proprietary technologies or has full administrator access to sensitive systems. |

ATTACHMENT 2: ITSP ACCESS/ACTION REQUEST FORM

**ITSP Request Form**

|  |  |
| --- | --- |
| Date:Requestor Name:Request Type:□ Information/Records□ Action | For Department:□ Human Resources□ Information Technology□ Legal□ Facility Security□ Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| DESCRIPTION OF REQUEST |
|  |
| REASON FOR REQUEST |
|  |
| PREREQUISITE REVIEWS/APPROVALS (IF APPLICABLE) |
| Department:Date:Representative: Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_----------------------------------------Department:Date:Representative: Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (FOR APPROVING DEPARTMENT) |
| Request: □ Approved □ DeniedRemarks:Date:Completed By: Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

ATTACHMENT 3: WORKPLACE SEARCH POLICY LETTER

**[Company] Search Policy**

The Company reserves the right to conduct searches to monitor compliance with rules concerning safety of employees, security of Company and individual property, drugs and alcohol, and possession of other prohibited items. "Prohibited items" includes illegal drugs, alcoholic beverages, prescription drugs or medications not used or possessed in compliance with a current valid prescription, weapons, any items of an unauthorized or violent nature, and any property in the possession or control of an employee who does not have authorization from the owner of such property to possess or control the property. "Control" means knowing where a particular item is, having placed an item where it is currently located, or having any influence over its continued placement. In addition to Company premises, the Company may search employees, their work areas, lockers, personal vehicles if driven or parked on Company property, and other personal items such as bags, purses, briefcases, backpacks, lunch boxes, and other containers. In requesting a search, the Company is by no means accusing anyone of theft, some other crime, or any other variety of improper conduct.

There is no general or specific expectation of privacy in the workplace of the Company, either on the premises of the Company or while on duty. In general, employees should assume that what they do while on duty or on the Company premises is not private. All employees and all of the areas listed above are subject to search at any time; if an employee uses a locker or other storage area at work, including a locking desk drawer or locking cabinet, the Company will either furnish the lock and keep a copy of the key or combination, or else allow the employee to furnish a personal lock, but the employee must give the Company a copy of the key or combination. The areas in question may be searched at any time, with or without the employee being present. As a general rule, with the exception of items relating to personal hygiene or health, no employee should ever bring anything to work or store anything at work that he or she would not be prepared to show and possibly turn over to Company officials and/or law enforcement authorities.

 All employees of the Company are subject to this policy. However, any given search may be restricted to one or more specific individuals, depending upon the situation. Searches may be done on a random basis or based upon reasonable suspicion. "Reasonable suspicion" means circumstances suggesting to a reasonable person that there is a possibility that one or more individuals may be in possession of a prohibited item as defined above. Any search under this policy will be done in a manner protecting employees' privacy, confidentiality, and personal dignity to the greatest extent possible. The Company will respond severely to any unauthorized release of information concerning individual employees.

I have received a copy of the Company’s Search Policy.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Signature |  | Date |
|  |  |  |
| Name |  |  |

ATTACHMENT 4: MONITORING RISK FLOWCHART



ATTACHMENT 5: INCIDENT RESPONSE TEAM - REPRESENTATIVES

|  |  |  |  |
| --- | --- | --- | --- |
| **DEPARTMENT/PERSONNEL** | **NAME** | **PHONE** | **E-MAIL** |
| ITPSO |  |  |  |
| Human Resources |  |  |  |
| Legal |  |  |  |
| Information Technologies |  |  |  |
| Facility Security |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

ATTACHMENT 6: ITPSO APPOINTMENT LETTER

<COMPANY LETTERHEAD>

|  |  |
| --- | --- |
| From: | [*Name*][*Title of Senior Company Official*] |
| Date: | [*Date*] |
| Re: | Insider Threat Program Senior Official Appointment Letter for [*Company*] |

Effective this date, [*Name of Appointee*], has been appointed as the Insider Threat Program Senior Official (ITPSO) for [*Company*] under CAGE: [*CAGE code*]. As the ITPSO they will be responsible for all duties and responsibilities as applicable to the position. Such responsibilities include the selection and endorsement of an Insider Threat Program Plan, as well as the implementation and execution of that plan.

[*Name of Signing Official*]

[*Title of Signing Official*]