

INSIDER THREAT POLICY

TABLE OF CONTENTS

1.	PURPOSE	2
2.	DEFINITIONS	2
3.	REFERENCES	2
4.	POLICY	2
4.2.	PURPOSE OF ITP	3
4.3.	INSIDER THREAT WORKING GROUP (ITWG).....	3
4.4.	ITP REQUIREMENTS.....	3
5.	RESPONSIBILITIES AND AUTHORITIES.....	3
5.1.	ITPSO.....	3
5.2.	ITWG.....	3
5.3.	EMPLOYEES (INCLUDING RESIDENT CONTRACTORS/SUBCONTRACTORS)	4
5.4.	MANAGERS	4
5.5.	EXECUTIVES	4
5.6.	DISTRIBUTION	4
5.7.	MAIN SAIL WEBSITE EMPLOYEE PORTAL	5
6.	POLICY OWNERSHIP	5
7.	MAIN SAIL REQUIREMENTS	5
7.1.	PERSONNEL TRAINING.....	5
7.2.	USER ACTIVITY	5
7.3.	TRACKING	5
7.4.	REPORTING REQUIREMENTS	6

1. Purpose

1.1.1. This Insider Threat Policy is created to implement an Insider Threat Program (ITP) that is consistent with 32 Code of Federal Regulation Part 117, National Industrial Security Program Operating Manual (NISPOM), also known as the “NISPOM rule.” which mandates that all cleared contractors establish and maintain an ITP that is an integrated departmental effort to deter, detect and mitigate risks by employees who may represent an insider threat to National Security and Main Sail.

2. Definitions

- **CNSI** – Classified National Security Information
- **CPI** – Company Proprietary Information
- **CSA** – Cognizant Security Agency
- **CUI** – Control Unclassified Information
- **DCSA** – Defense Counterintelligence and Security Agency
- **DD254** – DD Form 254 Contract Security Classification Specification
- **e-FCL** – Electronic Facility Clearance System
- **HR** – Human Resources
- **Insider Threat** – The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States and Main Sail
- **ISR** – Industrial Security Representative
- **IT** – Information Technology
- **ITP** – Insider Threat Program
- **ITPSO** – Insider Threat Program Senior Official
- **ITWG** – Insider Threat Working Group
- **KMP** – Key Management Personnel
- **NISPOM** – National Industrial Security Program Operating Manual
- **PII** – Personally Identifiable Information
- **SBU** – Sensitive But Unclassified

3. References

- 3.1. 32 CFR part 2004; E.O. 10865; E.O. 12333; E.O. 12829; E.O. 12866; E.O. 12968; E.O. 13526; E.O. 13563; E.O. 13587; E.O. 13691; Public Law 108–458; Title 42 U.S.C. 2011 *et seq.*; Title 50 U.S.C. Chapter 44; Title 50 U.S.C. 3501 *et seq.*
- 3.2. 32 Code of Federal Regulation Part 117, National Industrial Security Program Operating Manual (NISPOM), also known as the “NISPOM rule.” Sections: 117.7, 117.8, 117.12, 117.18

4. Policy

4.1.1. As a cleared defense contractor, Main Sail maintains a corporate wide Security Program that is compliant with 32 Code of Federal Regulation Part 117, National Industrial Security Program Operating Manual (NISPOM), also known as the “NISPOM rule.” This program will prevent espionage, violent acts against the Nation, or the unauthorized disclosure of classified information and controlled unclassified information; deter cleared employees from becoming insider threats; detect employees who pose a risk to classified information systems; and mitigate the risks to the security of classified information through administrative, investigative, or other responses. The ITP will meet or exceed the minimum standards for such programs, as defined in § 117.7 (d) of the NISPOM rule with additional guidance provided in Industrial Security Letter (ISL) 2016-02 and Defense Counterintelligence and Security Agency (DCSA) Assessment and Authorization Process Manual (DAAPM) under the NISPOM rule.

4.2. Purpose of ITP

4.2.1. The purpose of the ITP is to deter Main Sail employees and resident contractor/subcontractor personnel from becoming insider threats; detect insiders who pose a risk to classified national security information (CNSI), sensitive but unclassified (SBU), control unclassified information (CUI), personally identifiable information (PII), and company proprietary information (CPI); and mitigate the risk of an insider threat.

4.3. Insider Threat Working Group (ITWG)

4.3.1. The formation of an ITWG representing Information Technology (IT), Human Resources (HR), Legal/Contracts, Accounting, and Security will represent an integrated capability to access, share, and report information and data derived from offices and departments across Main Sail that are covered by any of the 13 personnel security adjudicative guidelines that is indicative of a potential or actual insider threat.

4.4. ITP Requirements

- The ITP will comply with the requirements and minimum standards of the 32 Code of Federal Regulation Part 117 *Insider Threat Program*, to include, but not limited to:
- Designate an Insider Threat Program Senior Official (ITPSO)
- Create an Insider Threat Working Group (ITWG)
- Conduct self-assessments of the ITP.
- Provide Insider Threat Awareness Training to all personnel.
- Monitor user activity on classified information systems.
- Monitor user activity on unclassified computer networks.
- Gather information for centralized analysis, reporting, and response capability.

5. RESPONSIBILITIES AND AUTHORITIES

5.1. ITPSO

5.1.1. The designated ITPSO must be a US citizen, senior official, cleared to the level of the facility clearance, and a Key Management Personnel (KMP) in the Electronic Facility Clearance System (e-FCL) for each cleared facility. Responsibilities to include:

- Provide management, accountability, and general oversight of the ITP.
- Ensure the close coordination of efforts across departments.
- Chair the ITWG meetings.

5.2. ITWG

5.2.1. The ITWG representing IT, HR, Legal/Contracts, Accounting, and Security will have responsibilities limited to their subject matter expertise:

5.2.2. **IT** – ensure the security and safety of Main Sail unclassified computer networks by establishing an integrated capability to monitor and audit user activity across all domains to detect and mitigate activity indicative of insider threat behavior and sharing suspicious activity with authorized ITP personnel.

5.2.3. **HR** – facilitate the sharing of applicable HR information with authorized ITP personnel, consistent with law and policy, that allows recognition of activity indicative of insider threat behavior (e.g. personnel related information such as; background results, drug screen results, performance

management, questionable outside work activities, membership of any hostile or anti-establishment organizations, signs of disgruntlement, disciplinary actions, etc.)

5.2.4. **Legal/Contracts** – review the ITP for legality and consistency with Executive Order 13587; protect the privacy and civil liberties of Main Sail personnel; provide legal support and advice to the ITWG.

5.2.5. **Accounting** – responsible for monitoring for unusual or excessive purchases, unusual accounting activity, and reporting wage garnishments to authorized ITP personnel.

5.2.6. **Security** – responsible for providing security-related information (facility access records, adverse information, security incident reports, security clearance adjudications, polygraph results, foreign travel/contacts) with authorized ITP personnel, and monitoring classified systems in order to detect activity indicative of insider threat behavior.

5.2.7. Core requirements of the ITWG include:

- Identify and prioritize what needs protection.
- Establish a centralized analysis and reporting procedure to document information that has been gathered that is indicative of insider threat behavior.
- Protect the information, documents, files, and material gathered in accordance with current federal laws, rules, and regulations.
- Assist with the development, implementation, and revision of procedures to ensure that all ITP activities, to include training, are conducted in accordance with applicable laws, whistleblower protections, civil liberties, and privacy policies.

5.3. EMPLOYEES (INCLUDING RESIDENT CONTRACTORS/SUBCONTRACTORS)

5.3.1. Shall comply with the requirements of current and applicable federal laws, rules, regulations, contract DD254s, Main Sail policies concerning the responsible sharing and safeguarding of CNSI, SBU, CUI, PII, and CPI, and all Client location security policies concerning security.

5.3.2. Shall report to the appropriate ITP personnel all contacts, activities, indicators, or behaviors that they observe, or gain knowledge, which could adversely impact the responsible sharing and safeguarding of CNSI, SBU, CUI, PII, and CPI

5.3.3. Shall not obstruct or impede any employee or other person from reporting a suspicious contact, activity, indicator, or behavior.

5.4. MANAGERS

5.4.1. All Managers shall support the ITWG in executing and implementing the Main Sail ITP with Main Sail employees and resident contractors/subcontractor personnel.

5.5. EXECUTIVES

5.5.1. All Executive personnel will ensure an integrated Company effort is maintained in support of the ITP.

5.6. DISTRIBUTION

5.6.1. The Insider Threat Policy will be distributed to all Main Sail employees and resident contractor/subcontractor personnel.

5.7. MAIN SAIL WEBSITE EMPLOYEE PORTAL

5.7.1. This Insider Threat Policy will be distributed during Onboarding. All staff will be sent a copy or link during onboarding.

6. Policy Ownership

6.1.1. This Insider Threat Policy is a Security level policy and approved by the Facilities Security Officer.

7. Main Sail Requirements

7.1. PERSONNEL TRAINING

7.1.1. All Cleared personnel are required to take Insider Threat Awareness training at [Training \(cdse.edu\)](http://Training(cdse.edu)). Certificates will be obtained and kept on file upon completion. Annual Refreshers of most current training available will be required.

7.1.2. Training records will be generated and kept on the S4/training records site. [Procedures - Training Records & Documents - Sorted by Status \(sharepoint.com\)](#)

7.2. USER ACTIVITY

7.2.1. Main Sail has user activity monitoring on information systems to detect activity indicative of insider threat behavior. These monitoring activities are performed at the system level and monitored by the IT Manager and 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 § 117.18 (a)(2) and (b)(4).

7.2.2. While Main Sail does not currently maintain classified information, all personnel are required to follow requirements at all Government or client sites where they may have access to or be in direct contact with classified or sensitive information. All personnel are subject to the location's policies as well as Main Sail's.

7.2.3. Main Sail's network is monitored for inappropriate access via the websites and has specific login and access security limitations by department for both our internet and intranet login.

7.2.4. Main Sail's access passwords have character minimum requirements and require reset every 120 days. In addition, they must be at least 9 characters long and cannot reuse last 12 passwords.

7.2.5. Main Sail monitors all internet activity in/out of the area.

7.2.6. Main Sail monitors all SharePoint activity in/out of the area.

7.2.7. Main Sail monitors all attempts to access the system - successful/unsuccessful.

7.2.8. Main Sail monitors all security changes.

7.2.9. Access to files/documents are granted on a need-to-know basis.

7.3. TRACKING

7.3.1. Main Sail has established procedures in accordance with 32 CFR §117.8 (c)(1), ISL 2006-02, and ISL 2011-4, 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.

7.3.2. Incidents that constitute suspicious contacts, in accordance with 32 CFR §117.8 (c)(2) and ISL 2006-02.

7.3.3. Main Sail tracks and provides a monthly report of network attack activities and reports accordingly.

7.3.4. Main Sail has implemented an internal database for security staff tracking of all reported events to allow for tracking and trend analysis of all issues, and flow through reporting agencies.

7.3.5. Each reported event will be entered into the ITP Database and kept on file indefinitely at [Admin - FSO Incident Tracker - All Items \(sharepoint.com\)](#)

7.3.6. No less than once per month, reporting will be generated from ITP Database and provided to DCSA Rep, CI rep, and FBI Rep with Monthly Network Attack Report.


- 7.3.7. Self-assessment records will be added to the Training Record Database for tracking and storage. [Procedures - Training Records & Documents - Sorted by Status \(sharepoint.com\)](#)
- 7.3.8. ITP records will be added to the Training Record Database for tracking and storage.

7.4. REPORTING REQUIREMENTS

- 7.4.1. All credible Insider Threat Information will be coordinated and shared with the ITPSO, which will then take action as directed in with 32 CFR 117.8, SEAD 3.”
The following information will be reported:
 - 7.4.2. Information regarding cleared employees, to include information indicative of a potential or actual insider threat and which falls into one of the 13 adjudicative guidelines, which must be reported when that information constitutes adverse information.
 - 7.4.3. Incidents that constitute suspicious contacts.
 - 7.4.4. 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 32 CFR 117, SEAD 3.
 - 7.4.5. Information determined to be any possible or potential successful penetration of a classified information system must be reported immediately in accordance with 32 CFR 117, SEAD 3.
 - 7.4.5.1. CI rep: Henderson, Andrew C andrew.c.henderson2.civ@mail.mil. DCSA / NAESOC Rep.
 - 7.4.5.2. Assistance with contacts and information for Counterintelligence: Defense Counterintelligence and Security Agency (DCSA) PO Box 644 Hanover, MD, 21076, Ph 1888-282-7682. General helpdesk: dcsa.naesoc.generalmailbox@mail.mil

ITPSO Assigned to Thelma Phillips, FSO Insider Threat Training. <http://cdsetrain.dtic.mil/itawareness/>.
Insider Threat Program Senior Official (ITPSO) Training Completed 09/14/2016

If a New ITPSO is appointed after the 6-month implementation period, the new ITPSO will complete the required training within 30-days of being assigned ITPSO responsibilities.


Thelma Phillips
FSO / ITPSO
9/17/2016

Brian Conley
Managing Partner

Contact list:
FSO/ITPSO Thelma Phillips
Assistant FSO Cynthia Gravelsins
HR Manager Thelma Phillips
Accounting Judy Stefanik
Contracts Thelma Phillips
IT Director Marc Phillips
(SMO) Managing Partner Brian Conley



Corporate Headquarters
8279 Mayfield Road, Unit #12
Chesterland, OH 44026
phone: (216) 472-5100
www.mainsailgroup.com

Change Log

Date	Name	Description
01/24/2024	Thelma Phillips, FSO	Update clause reference to 32 CFR 117, SEAD 3, added change log
01/26/2024	Thelma Phillips, FSO/ITPSO	Update signature block to include SMO, Reference information, Definition information.