Government/Commercial/Industrial Facilities & Security Services
5729 Leopard, Bldg. 8 Corpus Christi, TX. 78408 Off. 361-299-6767 Fax: 361-299-6769

SEC-OPS POLICY AND PROCEDURE

Insider Threat Program

1. Purpose. This Policy and Procedure establishes Sec-Ops policy and assigns responsibilities for the Insider Threat Program (ITP). The Insider Threat Program seeks to establish a secure operating environment for Sec-Ops personnel, systems, and facilities from insider threats.

2. **Background.** Executive Order (E.O.) 13587 signed into law on October 7, 2011, establishing new Governmentwide requirements to improve responsible sharing and safeguarding of classified information on computer systems. Additional guidance is found in the NISPOM requiring cleared contractors to establish Insider Threat Programs that deter, detect, and mitigate actions by employees who may represent a threat to national security.

3. **Scope and applicability.** This Policy and Procedure applies to all Sec-Ops staff personnel and offices and all Sec-Ops personnel who have access to or are eligible to access classified information and classified information systems. Sec-Ops personnel shall include employees and subcontractors with authorized access to Sec-Ops information and systems.

4. **Implementation.** This Sec-Ops Policy and Procedure is effective immediately and will be reviewed and updated as needed / required or every other year whichever is earlier. The Chief Executive Officer shall take all necessary actions to implement the designation herein.

.

5. **Sec-Ops Policy Guiding Principles.**

a. Sec-Ops is a cleared industry contractor and is subject to insider threats. Sec-Ops and all its personnel will take actions to mitigate or eliminate those threats.

b. Sec-Ops will continually identify and assess threats to the organization and its personnel and institute programs to defeat the threats.

c. Sec-Ops will leverage best practices used by the U.S. Intelligence Community and other Government agencies that operate counterintelligence programs and implement
them as necessary.

7. Policy.

a. The ITP is established as a Sec-Ops program to protect all Sec-Ops personnel, our facilities, automated systems and our clients from insider threats. This program is designed for establishing behaviors that improve our security vulnerability and assist to prevent espionage, violent acts against Sec-Ops, our clients, and the Government. It also assists in preventing the unauthorized disclosure of classified information; deter cleared employees from becoming insider threats; detect any employees who pose a risk to classified information systems and classified information; and helps to mitigate the risks to the security of classified information through administrative, investigative, or other responses.

b. The Sec-Ops ITP shall meet or exceed the minimum standards for such programs, as defined in the NISPOM.

c. The responsibilities outlined below are designed to enable the ITP to gather, integrate, centrally analyze, and respond appropriately to key threat-related information.
The ITP shall consult with our records management, legal counsel, and the Hr department 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.
a. All Sec-Ops departments and personnel are responsible for fully supporting the intent and requirements of the ITP and:

(1) The CEO is appointed as the ITP Program Lead who will act as the corporate representative for Sec-Ops and all ITP implementing activities;

(2) Maintaining all associated records and submitting required reports to the FSO;

(3) Enforcing requirements to support the Insider Threat and the related training programs;

(4) Enforcing Sec-Ops Foreign Travel, Meeting and Foreign Visitor Programs for the purpose of tracking, documenting, and retrieving relevant information on cleared employee foreign travel, meetings, and foreign visitor contacts;

(5) Ensuring responsible sharing of all required information pertaining to personnel, systems, and activities in accordance with applicable laws, privacy policies and civil liberties policies, with designated ITP personnel conducting activities under the ITP.

b. Sec-Ops Managers. Each manager is responsible for fully supporting the intent and requirements of the ITP and:

(1) Enforcing requirements to support the Insider Threat and the related training programs;

(2) Enforcing Sec-Ops Foreign Travel, Meeting, and Foreign Visitor Programs for the purpose of tracking, documenting, and retrieving relevant information on cleared employees' foreign travel, meetings, and foreign visitor contacts;

(3) Ensuring responsible sharing of all required information pertaining to personnel, systems, and activities in accordance with applicable laws and policy with designated Insider Threat personnel conducting activities under the ITP.

c. Senior Official for Insider Threat. The CEO of Sec-Ops is appointed as the designated Senior Official for the Insider Threat Program. Responsibilities include:

(1) Leading Sec-Ops in establishing, implementing, and overseeing the activities of the ITP;

(2) Ensuring the program is executed in accordance with all applicable laws and privacy policies;

(3) Establishing guidelines and procedures for the retention, sharing, and safeguarding of records and documents necessary to complete inquiries and assessments;

(4) Establishing and leading an ITP Core Coordination Council for consultation on all ITP-related issues, conducting program oversight and reviews, as well as identifying and making program resource recommendations. At a minimum, the Sec-Ops committee will be comprised of the Administrative Director, the Human Resources Manager, the FSO or assistant, the Information Assurance Manager, and the Chief Financial Officer;

(5) Establishing an ITP activity with a centralized analysis and response capability to manually and/or electronically gather, integrate, review, assess and respond to information derived from Counterintelligence, Information Assurance, Security, Human Resources, the monitoring of user computer activity, and other information sources as deemed appropriate;

(6) Overseeing the collection, analysis, and reporting of information throughout Sec-Ops to support the identification and assessment of insider threats;

(7) Establishing and managing all implementation and reporting requirements, to include self-assessments and independent assessments, the results of which shall be reported to the CEO and Committee;

(8) Ensuring the ITP establishes procedures for insider threat response action(s) to clarify or resolve insider threat matters. Those procedures will ensure that response action(s) are centrally managed and documented;

(9) Leading the establishment and execution of an Insider Threat Awareness
Training Program in accordance with the NISPOM Insider Threat Policy; and

(10) Detailing or assigning cleared staff, as appropriate and necessary, to the Program.

d. The Human Resources Manager is responsible for:
(1) Is appointed to coordinate with the Administrative Director of on all matters related to the sharing of all relevant personnel records, to support the identification, analysis, assessment, and resolution of any potential insider threat matter; and

(2) Implementing policies and procedures to inform Sec-Ops employees as to the existence of the ITP.

e. The Chief Financial Officer is responsible for:
Appointed to coordinate with the Administrative Director on all matters related to the sharing of all relevant financial records, to support the identification, analysis, assessment, and resolution of any potential insider threat matter;

f. The Sec-Ops General Counsel is responsible for:
(1) Providing legal advice for the establishment, implementation, execution, management, and oversight of the ITP; and

(2) Providing legal review of all responses to any inquiries stemming from the execution of the ITP.

g. The IA Manager is responsible for:

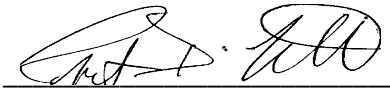
(1) Appointed to coordinate with the committee on all matters related to the sharing of all relevant Information Technology/Information Assurance records/monitoring, to support the identification, analysis, assessment, and resolution of any potential insider threat matter;

(2) Establishing and enforcing an information system protection program to identify system security threats, vulnerabilities, and mitigation strategies; and

(3) Establishing a comprehensive user awareness program to inform Sec-Ops personnel of IA system monitoring and auditing.

h. **The FSO/Assistant FSO role:**

All credible Insider Threat Information will be coordinated and shared with the FSO and/or the assistant FSO, which will then take action as the CEO deems appropriate, including coordinating with law enforcement agencies, such as the Federal Bureau of Investigation.



July 28, 2016

Robert D. Lott
CEO
Sec-Ops, Inc.

Date

Appendix A. Reference and Authorities List
Appendix B. Definitions
Appendix C. Reporting Requirements

Appendix A. Reference and Authorities List

The following list of references and authorities should be used in developing, implementing, and executing the overall Insider Threat Program and any supporting sub-programs. This list will be reviewed and updated as required or at 2-year intervals, whichever is earlier:

Public Laws:
National Security Act of 1947, 50 U.S.C. § 3002, *et seq*.
Counterintelligence Enhancement Act of 2002, 50 U.S.C. § 3382, *et seq* .
Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C § 3002, *et seq*.

Executive Orders:
E.O. 12968, Access to Classified Information, August 4, 1995.
E.O. 12829, National Industrial Security Program, January 6, 1993, as amended.
E.O. 13526, Classified National Security Information, December 29, 2009.
E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011.

Presidential Directives:
Presidential Decision Directive PDD/NSC-12 Security Awareness and Reporting of Foreign Contacts, August 5, 1993.
November 21, 2012 Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

Governing Document:
DoD 5220.22-M, "National Industrial Security Program Operating Manual," as amended

Sec-Ops Policies & Procedures:
Sec-Ops Policy of Business Ethics
Sec-Ops Policy Manual
Sec-Ops Information Technology (IT) Security Policy
Sec-Ops Information Technology (IT) Rules of Behavior
Sec-Ops Privacy Act Policy
Sec-Ops Suitability and Personnel Security Program

Appendix B. Definitions

Agencies: Pursuant to section 7 of E.O. 13587, the term “agencies” has the meaning set forth in section 6.1 (b) of E.O. 13526, which includes any “executive agency” as defined in 5 U.S.C. 105 and “any other entity within the executive branch that comes into the possession of classified information.”

Classified information: Information that has been determined pursuant to E.O. 13526, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

Employee: For purposes of this policy, "employee" has the meaning provided in section 1.1(e) of E.O. 12968; specifically: a person, other than the President and Vice President, employed by, detailed or assigned to Sec-Ops; an expert or consultant to Sec-Ops; an industrial or commercial subcontractor, licensee, certificate holder, or grantee of Sec-Ops, including all subcontractors; or any other category of person who acts for or on behalf of Sec-Ops as determined by the CEO.

Insider: Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.

Insider Threat: The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States or Sec-Ops. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of Sec-Ops resources or capabilities.

Government/Commercial/Industrial Facilities & Security Services
5729 Leopard, Bldg. 8 Corpus Christi, TX. 78408 Off. 361-299-6767 Fax: 361-299-6769

Appendix C

CLEARED EMPLOYEE REPORTING REQUIREMENTS

As an individual who has been granted a security clearance by Sec-Ops, you are required to report the following issues to the FSO or Assistant FSO Immediately. *Robert@secopsinc.com 361-688-4127 0r victor@secopsinc.com 307-275-2205*.

1. Adverse Information

Adverse information is any information that adversely reflects on the integrity or character of a cleared employee, which suggests that his/her ability to safeguard classified information may be impaired, or that his/her access to classified information clearly may not be in the interests of national security. You must report the following types of information about yourself or other employees:

- Arrests or convictions for criminal offenses including drunk driving and traffic violations over $300;
- Financial difficulties, including bankruptcy, excessive indebtedness, and wage garnishments;
- Aberrant behavior;
- Alcoholism, use of illegal drugs, or abuse of legal drugs;
- Emotional or psychological problems requiring treatment or hospitalization;
- Affluence (wealth, acquisitions, investments) beyond known sources of income.

2. Change in Personal Status

You must report:

- A change in name;
- A change in marital status (i.e., marriage or divorce);
- A change in citizenship;
- When access to classified information is no longer required due to a change in job assignments.

3. Foreign Contact/Foreign Travel

You must report any close and continuing contact with a foreign national. You must report when you begin to act as a representative of or consultant to any foreign entity, including a government, a government agency, a commercial business, or a person. You must report all personal and official foreign travel.

4. Security Incidents/Violations

You must report any known or suspected security violation or vulnerability of which you become aware, independent of who is responsible or at fault for the situation. Security violations/vulnerabilities include:

- The careless or unintentional failure to comply with security requirements for safeguarding classified information;
- The intentional disregard of security requirements;
- Any failure to comply with security requirements, regardless of intent, that has resulted in the loss, compromise, or suspected compromise of classified information;
- The unauthorized receipt of classified material;
- Significant vulnerabilities discovered in equipment or systems designed to protect classified information.

5. Espionage, Sabotage, Subversive Activities

You must immediately report any situation related to actual, probable, or possible espionage, sabotage, or subversive activities directed at the United States.

6. Suspicious Contacts

You must report:

- Any efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise any cleared employee;
- Any contact by a cleared employee with known or suspected intelligence officers from any country;
- Any contact which suggests you or another employee may be the target of an attempted exploitation by the intelligence services of another country.

Government/Commercial/Industrial Facilities & Security Services
5729 Leopard, Bldg. 8 Corpus Christi, TX. 78408 Off. 361-299-6767 Fax: 361-299-6769

INSIDER THREAT

REPORTABLE BEHAVIORS

All individuals employed by or with Sec-Ops must immediately report any of the following activities, indicators, or behaviors to the Sec-Ops FSO or Assistant FSO at (361) 299-6767 or (307) 275-2205.

Table 1. Reportable Contacts, Activities, Indicators, and Behaviors

1.	When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against facilities, organizations, personnel, or information systems. This includes contact through social networking sites that is not related to official duties.
2.	Attempts by anyone, regardless of nationality, to obtain or acquire unauthorized access to classified or sensitive information in the form of facilities, activities, personnel, technology or material through any of the following methods: questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence (including electronic correspondence) or automated systems intrusions.
3.	Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
4.	Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
5.	Acquiring, or permitting others to acquire, unauthorized access to classified information systems.
6.	Attempts to obtain classified information by an individual not authorized to receive such information.
7.	Persons attempting to obtain access to information inconsistent with their duty requirements.
8.	Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.
9.	Discovery of suspected listening or surveillance devices in classified or secure areas.
10.	Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
11.	Discussions of classified information over a non-secure communication device.
12.	Reading or discussing classified information in a location where such activity is not permitted.
13.	Transmitting or transporting classified information by unsecured or unauthorized means.
14.	Removing or sending classified material out of secured areas without proper authorization.
15.	Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.
16.	Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.
17.	Improperly removing classification markings from documents or improperly changing classification markings on documents.
18.	Unwarranted work outside of normal duty hours.
19.	Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.
20.	Attempts to entice personnel or contractors into situations that could place them in a compromising position.

21.	Attempts to place personnel or contractors under obligation through special treatment, favors, gifts, or money.
22.	Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
23.	Requests for information that make an individual suspicious, to include suspicious or questionable requests over the internet or social networking sites.
24.	Trips to foreign countries that are: a. Short trips inconsistent with logical vacation travel or not part of official duties. b. Trips inconsistent with an individual's financial ability and official duties.
25.	Personnel who are in contact with any official or citizen of a foreign country when the foreign official or citizen: a. Exhibits excessive knowledge of or undue interest in personnel or their duties beyond the normal scope of friendly conversation. b. Attempts to obtain classified or unclassified information. c. Attempts to place personnel under obligation through special treatment, favors, gifts, money or other means. d. Attempts to establish business relationships that are outside the scope of normal official duties.
26.	Incidents in which personnel or their family members traveling to or through foreign countries are contacted by persons who represent a foreign law enforcement, security or intelligence organization and a. Are questioned about their duties. b. Are requested to provide classified or unclassified information. c. Are threatened, coerced or pressured in any way to cooperate with the foreign official. d. Are offered assistance in gaining access to people or locations not routinely afforded Americans.
27.	Unexplained or undue affluence. a. Expensive purchases an individual's income does not logically support. b. Attempts to explain wealth by reference to inheritance luck in gambling, or a successful business venture. c. Sudden reversal of a bad financial situation or repayment of large debts.
28.	Contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which: a. Illegal or unauthorized access is sought to classified or otherwise sensitive information. b. The employee is concerned that he/she may be the target of actual or attempted exploitation by a foreign entity.
29.	Any contact with the media where the media seeks access to or results in the unauthorized disclosure of classified information, unclassified, or other information not approved for public release.
30.	Arrests, charges, convictions, and criminal court appearance (with the exceptions of a summons for jury duty or to appear as a witness or provide other testimony when the individual is not being charged or otherwise being prosecuted). Traffic infractions where the fine was less than $300 and did not involve alcohol or drugs are not reportable. All reports should include dates, jurisdiction, name of the court, nature of the issue, and disposition, if available. Changes in the status of any previously reported court involvement shall also be promptly reported.
31.	Adverse changes to financial status to include, but not limited to, garnishments, foreclosures, liens, judgments, delinquent taxes, and/or bankruptcy filings.
32.	Any hospitalization for a mental health condition.
33.	Use of or involvement with illegal drugs or controlled substances, and/or the misuse of prescription/legal drugs or dangerous inhalants.
34.	Voluntary or involuntary treatment for abuse of alcohol or illegal use of controlled substances.

35.	Close and continuing association with foreign nationals.
36.	Unwillingness to comply with rules and regulations, or to cooperate with security requirements.
37.	Alcohol abuse.
38.	Apparent or suspected mental or emotional condition where there is reason to believe the condition may affect the individual's judgment, reliability, or ability to protect classified information.
39.	Criminal conduct.
40.	Any activity that could constitute a conflict of interest with U.S. Government employment.
41.	Misuse or abuse of U.S. Government property or information systems.

Table 2. Reportable Suspected Terrorism or Work Place Violence Contacts, Activities, Indicators, and Behaviors

1.	Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.
2.	Advocating support for a known or suspected international terrorist organizations or objectives.
3.	Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
4.	Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
5.	Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.
6.	Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.
7.	Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.
8.	Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
9.	Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.
10.	Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.
11.	Possessing weapons in the work place.
12.	Threatening to kill or harm supervisors, co-workers or anyone else within or outside of the work place.
13.	Sending emails or posting on social media sites threatening communications against supervisors, co-workers or anyone else within or outside of the work place.

Table 3. Reportable Behaviors Associated With Cyberspace Contacts, Activities, Indicators

1.	Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of U.S. Government information.
2.	Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3.	Network spillage incidents or information compromise.
4.	Use of account credentials by unauthorized parties.
5.	Tampering with or introducing unauthorized elements into information systems.
6.	Unauthorized downloads or uploads of sensitive data.
7.	Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8.	Downloading or installing non-approved computer applications.
9.	Unauthorized network access.
10.	Unauthorized e-mail traffic to foreign destinations.
11.	Denial of service attacks or suspicious network communications failures.
12.	Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13.	Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14.	Data ex-filtrated to unauthorized domains.
15.	Unexplained storage of encrypted data.
16.	Unexplained user accounts.
17.	Hacking or cracking activities.
18.	Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19.	Malicious codes or blended threats such as viruses, worms, Trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.