

**STANDARD PRACTICES AND PROCEDURES (SPP)
FOR PERSONNEL SECURITY AND INSIDER THREAT**



**201 King St. #201
Alexandria, VA 3314**

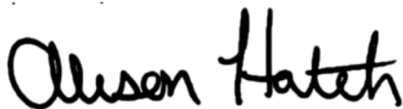
Forward

Riptide Technology, Inc., henceforth referred to as 'Riptide Technology', has entered into a Security Agreement with the Department of Defense in order to have access to information that has been classified because of its importance to our nation's defense.

Some of our programs and activities are vital parts of the defense and security systems of the United States. All of us – both management and individual employees – are responsible for properly safeguarding the classified information entrusted to our care.

Our Standard Practice Procedures conforms to the security requirements set forth in the government manual – the National Industrial Security Program Operating Manual or NISPOM. The purpose of our SPP is to provide our employees with the requirements of the NISPOM as they relate to the type of work we do. This document should also serve as an easy reference when questions about security arise. The NISPOM is available for review by contacting the Facility Security Officer.

Our company fully supports the National Industrial Security Program. All of us have an obligation to ensure that our security practices contribute to the security of our nation's classified defense information.

A handwritten signature in black ink that reads "Alison Hatch". The signature is written in a cursive, flowing style. Below the signature is a solid blue horizontal line.

ALISON E HATCH

President and Facility Security Officer

Table of Contents

1. Introduction	1
2. Facility Information	1
2.1. Facility Clearance	1
2.2. Facility Security Officer	1
2.3. Insider Threat Program Senior Official	1
2.4. Storage Capability	1
3. Personnel Security Clearances.....	1
3.1. Clearance Procedures	1
3.2. Reinvestigations	2
3.3. Consultants	2
4. Security Education	2
4.1. Security Briefings	2
4.2. Insider Threat Briefings.....	3
4.3. Debriefings	3
4.4. Derivative Classification Training.....	3
5. Security Vulnerability Assessments/Self-Inspections	3
5.1. Defense Security Service.....	3
5.2. Security Vulnerability Assessments (SVA)	3
5.3. Self-Inspections.....	3
6. Individual Reporting Responsibilities	4
6.1. Espionage/Sabotage	4
6.2. Suspicious Contacts.....	4
6.3. Adverse Information	4
6.4. Loss, Compromise, or Suspected Compromise of Classified Information.....	4
6.5. Security Violations	4
6.6. Personal Changes.....	5
6.7. Security Equipment Vulnerabilities	5
6.8. Foreign Travel	5
7. Disciplinary Actions	5

8. Defense Hotline	6
9. Marking Classified Information	6
9.1. Classification Levels	6
9.2. Original Classification	6
9.3. Derivative Classification	6
10. Classified Information	6
10.1. Classification Levels	6
10.2. Classified Information at Riptide Technology	7
11. Public Release/Disclosure	7
12. Insider Threat	7
12.1. Collect Personnel Security Information	7
12.2. Evaluate Personnel Security Information	7
12.3. Provide Insider Threat Awareness Training	7
13. Definitions	8
14. Abbreviations & Acronyms	9
15. References	10

1. Introduction

This Standard Practices and Procedures (SPP) describes Riptide Technology policies regarding the handling and protection of classified information. This SPP is applicable to all employees, subcontractors, consultants, vendors, and visitors to our facility and is a supplement to the National Industrial Security Program Operating Manual (NISPOM)^[1], which takes precedence in instances of apparent conflict.

2. Facility Information

2.1. Facility Clearance

A facility clearance (FCL) is an administrative determination that a facility is eligible for access to classified information or award of a classified contract. Riptide Technology has a Top Secret facility clearance. The FCL is valid for access to classified information at the Top Secret or lower classification level.

2.2. Facility Security Officer

Having a facility clearance Riptide Technology must agree to adhere to the rules of the National Industrial Security Program (NISP). As part of the NISP, contractors are responsible for appointing a Facility Security Officer (FSO). The FSO must be a U.S. citizen, an employee of the company, and cleared to the level of the facility clearance. The FSO must complete required training and is responsible for supervising and directing security measures necessary for implementing the NISPOM and related Federal requirements for classified information. Alison Hatch is the FSO for Riptide Technology and can be reached at 703-888-2711 or by e-mail at ahatch@riptide-tech.com

2.3. Insider Threat Program Senior Official

Adherence to the NISP includes maintaining a program to identify and defeat insider threats. The FSO for Riptide Technology will also serve as the Insider Threat Program Senior Official (ITPSO). The ITPOS will be designated in writing and will act as the company's representative for Insider Threat Program activities. The ITPSO will be cleared in connection with the facility clearance, be a United States citizen, and will be designated as Key Management Personnel (KMP) in e-FCL in accordance with Cognizant Security Agency (CSA) guidance and in accordance with NISPOM 1-202b.

2.4. Storage Capability

The facility clearance level is separate from the storage capability level. Contractors must receive a separate approval prior to storing any classified information. Riptide Technology has **NOT** been approved to store any classified.

3. Personnel Security Clearances

3.1. Clearance Procedures

Riptide Technology employees will be processed for a personnel security clearance (PCL) only when a determination has been made that access is necessary for performance on a classified contract. The

number of employees processed for a clearance will be limited to the minimum necessary for operation efficiency.

Riptide Technology will utilize the Joint Personnel Adjudication System (JPAS) to initiate the clearance request process. Each applicant for a security clearance must produce evidence of citizenship such as an original birth certificate or passport. Applicants will complete the Questionnaire for National Security Positions (SF-86) through OPM's electronic questionnaires for investigation processing (e-QIP) system.

The FSO will ensure that prior to initiating the e-QIP action, the applicant is provided a copy of NISPOM paragraph 2-202. This ensures the employee is aware that the SF-86 is subject to review by the FSO only to determine the information is adequate and complete but will be used for no other purpose and protected in accordance with the Privacy Act of 1975.

While Riptide Technology initiates the clearance process for employees, the government will make the determination of whether or not an individual is eligible to access classified information and grant the personnel clearance.

3.2. Reinvestigations

Depending upon the level of access required, individuals holding security clearances are subject to a periodic reinvestigation (PR) at a minimum of every five years for Top Secret, 10 years for Secret and 15 years for Confidential. Our FSO is responsible for reviewing all access records to ensure employees are submitted for PRs as required.

3.3. Consultants

For security administration purposes, consultants are treated as employees of Riptide Technology and must comply with this SPP and the NISPOM. Consultants will, however, be required to execute a Consultant Agreement which outlines any security responsibilities specific to the consultant.

Note: If Riptide Technology sponsors a consultant for a PCL, Riptide Technology must compensate the consultant directly; otherwise, the company receiving compensation must obtain a Facility Security Clearance (FCL) and serve as a subcontractor to Riptide Technology.

4. Security Education

4.1. Security Briefings

All cleared employees must receive an initial security briefing and sign a Nondisclosure Agreement (SF 312) prior to being granted access to classified material for the first time. The SF 312 is an agreement between the United States and a cleared individual. At a minimum, the initial briefing will include the following:

- Threat Awareness Briefing
- Defensive Security Briefing
- Overview of Security Classification System
- Employee reporting obligations and requirements
- Overview of the SPP

The security briefings will be provided annually to all cleared employees in order to remind employees of their obligation to protect classified information and provide any updates to security requirements.

4.2. Insider Threat Briefings

All employees will receive Insider Threat Awareness training upon hiring and will be again be provided this training annually.

4.3. Debriefings

When a cleared employee no longer requires a security clearance or terminates employment with Riptide Technology, the employee will be debriefed by the FSO.

4.4. Derivative Classification Training

Riptide Technology employees who have been authorized to make derivative classification decisions must complete initial derivative classification training and refresher training at least once every 2 years before being authorized to make derivative classification decisions. Documentation will be retained identifying the date of the most recent training and type of training derivative classifiers receive. Contact the FSO for guidance on how to access and complete the training.

5. Security Vulnerability Assessments/Self-Inspections

5.1. Defense Security Service

The Defense Security Service (DSS) is the government cognizant security office (CSO) which provides oversight of contractors' procedures and practices for safeguarding classified defense information. Industrial Security Representatives of DSS may contact you in connection with the conduct of a security vulnerability assessment of the facility, an investigation of an unauthorized disclosure of classified information, or to provide advice and assistance to you and Riptide Technology on security related issues.

Our assigned DSS field office is:

27130 Telegraph Road
Quantico, Virginia 22134
571-305-6751
571-305-6752

5.2. Security Vulnerability Assessments (SVA)

Riptide Technology may be assessed by the DSS on a 18-24 month cycle. During this time, DSS Industrial Security Representatives will review our security processes and procedures to ensure compliance with the NISPOM, and interview Riptide Technology employees to assess the effectiveness of the security program. Your cooperation with DSS during the SVA is required.

5.3. Self-Inspections

Riptide Technology security staff will also perform a self-inspection, similar to the DSS SVA. The purpose is to self-assess the security procedures to determine the effectiveness and identify any deficiencies/weaknesses. As part of this self-inspection, Riptide Technology employees will be interviewed. The results of the self-inspection will be briefed to employees during refresher briefings.

6. Individual Reporting Responsibilities

All Riptide Technology employees are to report any of the following information to the FSO. Our FSO Alison Hatch can be reached by e-mail at ahatch@riptide-tech.com. However, do not discuss sensitive or private issues via e-mail. Alert the FSO to the existence of an issue and provide contact information.

6.1. Espionage/Sabotage

Report any information concerning existing or threatened espionage, sabotage or subversive activities. The FSO will forward a report to the FBI and DSS via their hotline numbers.

6.2. Suspicious Contacts

Suspicious contacts are efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise cleared employees. Personnel should report all suspicious contacts to the FSO. The FSO forwards all reports to the respective government agency for review and action.

6.3. Adverse Information

Adverse information is any information regarding a cleared employee or employee in process for a clearance which suggests that his/her ability to safeguard classified information may be impaired or that his or her access to classified information may not be in the interest of national security. Cleared personnel report adverse information regarding himself, herself, or another cleared individual to the FSO. Reportable adverse information includes:

- Relationships with any known saboteur, spy, traitor, anarchist, or any espionage or secret agent of a foreign nation
- Serious mental instability or treatment at any mental institution
- Use of illegal substances or excessive use of alcohol or other prescription drugs
- Excessive debt, including garnishments on employee's wages
- Unexplained affluence/wealth
- Unexplained absence from work for periods of time that is unwarranted or peculiar
- Criminal convictions involving a gross misdemeanor, felony, or court martial
- Violations and deliberate disregard for established security regulations or procedures
- Unauthorized disclosure of classified information
- Members of, or individuals sympathetic to, an organization aiming to overthrow the U.S. Government by unconstitutional means.
- Involvement in the theft of, or any damage to, Government property

Note: Reporting adverse information does not necessarily mean the termination of a personnel clearance. Reports should not be based on rumor or innuendo.

6.4. Loss, Compromise, or Suspected Compromise of Classified Information

Cleared personnel must immediately report the loss, compromise, or suspected compromise of classified information.

6.5. Security Violations

Cleared personnel must report any failure to comply with a requirement of this SPP or of the NISPOM. See Section 7 regarding Riptide Technology's graduated scale of disciplinary actions.

6.6. Personal Changes

Cleared personnel report personal changes to include:

- Change in name
- Termination of employment
- Change in citizenship
- Access to classified information is no longer needed
- No longer wish to be processed for a personnel clearance or continue an existing clearance

6.7. Security Equipment Vulnerabilities

Personnel must report significant vulnerability in security equipment or hardware/software that could possibly lead to the loss or compromise of classified information.

6.8. Foreign Travel

Personnel must report all foreign travel, including itinerary, passport data, contact information, and planned foreign contacts, to the FSO at the earliest possible date. The FSO will provide individuals a travel briefing including Department of State country-specific concerns. Additionally, upon return from travel, personnel should again report to the FSO for a travel debrief. Foreign travel will be reported in the Defense Information System for Security.

7. Disciplinary Actions

Riptide Technology employees may only work with classified information at approved customer facilities. If an employee violates the security at a customer site, Riptide Technology will follow and enforce the disciplinary actions dictated by that customer's facility security officer. If administrative actions related to security violations result in an employee's inability to work at the customer facility, the employee may be terminated.

Employees who violate the security procedures are subject to the graduated scale of disciplinary actions as follows:

1. First violation within a period of 12 consecutive months — verbal reprimand and counseling by the FSO or the employee's immediate supervisor.
2. Second violation within a period of 12 consecutive months — written reprimand and verbal counseling by the FSO or the employee's immediate supervisor. Reprimand will be added to employee's personnel file.
3. Third violation within a period of 12 consecutive months — written reprimand and verbal counseling by the FSO or the employee's immediate supervisor. Reprimand will be added to employee's personnel file. Employee must document a written plan of action for avoiding further incidents that will also be added to employee's personnel file.

Deliberate incidents or incidents which involve gross negligence or a pattern of negligence will be reviewed on a case-by-case basis for appropriate disciplinary action and could result in termination of employment.

8. Defense Hotline

The Department of Defense (DoD) provides a Defense Hotline as a confidential avenue for individuals to report allegations of wrongdoing pertaining to programs, personnel, and operations that fall under the purview of the Department of Defense, pursuant to the Inspector General Act of 1978. Anyone, including members of the public, DoD personnel and DoD contractor employees, may file a complaint with the DoD Hotline.

DEFENSE HOTLINE
THE PENTAGON
WASHINGTON, DC 20301-1900
TELEPHONE: 800-424-9098
<http://www.dodig.mil/hotline>

9. Marking Classified Information

9.1. Classification Levels

- **TOP SECRET** - Material that if compromised could cause “Exceptionally Grave” damage to national security and requires the highest degree of protection.
- **SECRET** - Material that if compromised could cause “Serious” damage to national security and requires a substantial degree of protection.
- **CONFIDENTIAL** - Material that if compromised could cause “Identifiable” damage to national security.

9.2. Original Classification

The determination to originally classify information may be made ONLY by a U.S. Government official who has been delegated the authority in writing. Information is classified pursuant to Executive Order 13526 and is designated and marked as Top Secret, Secret or Confidential. Contractors make derivative classification decisions based on the guidance provided by the Contract Security Classification Specification (DD Form 254) and Security Classification Guidance applicable to each classified contract.

9.3. Derivative Classification

Riptide Technology employees authorized to perform derivative classification actions must have adequate training and the proper classification guides and/or guidance necessary to accomplish these important actions. See Section 4.4 regarding required derivative classification training.

10. Classified Information

10.1. Classification Levels

- **TOP SECRET** - Material that if compromised could cause “Exceptionally Grave” damage to national security and requires the highest degree of protection.
- **SECRET** - Material that if compromised could cause “Serious” damage to national security and requires a substantial degree of protection.

- **CONFIDENTIAL** - Material that if compromised could cause “Identifiable” damage to national security.

10.2. Classified Information at Riptide Technology

Classified information **CANNOT** be stored on the premises of Riptide. Classified information **CANNOT** be entered into any computer or other electronic device at Riptide Technology. Classified information **CANNOT** be discussed on the premises of Riptide.

11. Public Release/Disclosure

Riptide Technology is not permitted to disclose classified or unclassified information pertaining to a classified contract to the public without prior review and approval by the government customer. If you have a need to perform a presentation or create brochures, promotional sales literature, reports to stockholders, or similar materials, on subject matter related to a classified contract, even if unclassified, please see the FSO to determine if we must obtain approval from the customer.

Note: Classified information made public is not automatically considered unclassified. Riptide Technology personnel shall continue the classification until formally advised to the contrary.

12. Insider Threat

Riptide Technology is subject to insider threats and will take actions to mitigate or eliminate those threats. Riptide Technology will continually identify and assess threats to the organization and its personnel as well as institute programs to defeat the threats. The Insider Threat Program for Riptide Technology has three main components:

12.1. Collect Personnel Security Information

The Insider Threat Program Senior Official, with the assistance of Key Management Personnel, will collection and any all information that could indicate the existence of an insider threat. This information includes any reported by the individual as part of self-reporting (see Section 6). This information includes any disciplinary actions taken by management personnel. And this information includes other relevant information such as reports of outside employment, reports of strange or inappropriate behavior by coworkers, or and information from the Self-Reporting requirements that Riptide Technology becomes aware of from sources other than the individual. All of this information will be recorded and maintained in the employee personnel file at Riptide Technology corporate offices.

12.2. Evaluate Personnel Security Information

All key management personnel with access to employee personnel files are responsible for evaluating an employee’s file any time any information mentioned in the previous section is added to the file. If there is a body of evidence sufficient to warrant investigation of an insider threat, the key management personnel are responsible for reporting it to the government agency security office.

12.3. Provide Insider Threat Awareness Training

The ITPSO is responsible to providing Insider Threat Awareness Training to all employees when they are first hired and annually thereafter. The training will address current and potential threats in the work and personal environment and will include the following:

- The importance of detecting potential Insider Threats by cleared employees and reporting suspected activity to the Insider Threat Program designee.
- 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.
- Counterintelligence and security reporting requirements.

Riptide Technology does not maintain any classified information systems and, therefore, has no requirements for monitoring of such systems.

13. Definitions

The following definitions are common security related terms.

Access	The ability and opportunity to obtain knowledge of classified information.
Adverse Information	Any information that adversely reflects on the integrity or character of a cleared employee, which suggests that his or her ability to safeguard classified information may be impaired or that his or her access to classified information clearly may be in the interest of national security.
Authorized Person	A person who has a need-to-know for the classified information involved, and has been granted a personnel clearance at the required level.
Classified Contract	Any contract that requires, or will require, access to classified information by the contractor or its employees in the performance of the contract.
Classified Information	Official Government information which has been determined to require protection against unauthorized disclosure in the interest of national security.
Cleared Employees	All Riptide Technology employees granted a personnel clearance or who are in process for a personnel clearance.
Closed Area	An area that meets the requirements outlined in the NISPOM for safeguarding classified information that, because of its size, nature, and operational necessity, cannot be adequately protected by the normal safeguards, or stored during nonworking hours in approved containers.
Communication Security (COMSEC)	COMSEC refers to protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications.
Compromise	An unauthorized disclosure of classified information.
CONFIDENTIAL	Classified information or material that requires protection whereby unauthorized disclosure could reasonably be expected to cause damage to our national security.
Facility (Security) Clearance	An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).
Foreign Interest	Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its territories, and any person who is not a citizen or national of the United States.
Foreign National	Any person who is not a citizen or national of the United States.
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 security of the United States
Need-to-Know (NTK)	A determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services to fulfill a classified contract or program.
Personnel Security Clearance (PCL)	An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

Public Disclosure	The passing of information and/or material pertaining to a classified contract to the public or any member of the public by any means of communication.
SECRET	Classified information or material that requires a substantial degree of protection, the unauthorized disclosure of which could reasonably be expected to cause serious damage to our national security.
Security Violation	Failure to comply with policy and procedures established by the NISPOM that could reasonably result in the loss or compromise of classified information.
Standard Practice Procedures (SPP)	A document prepared by contractors outlining the applicable requirements of the NISPOM for the contractor's operations and involvement with classified information at the contractor's facility.
Subcontractor	A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor.
TOP SECRET	Classified information or material that requires the highest degree of protection, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to our national security.
Unauthorized Person	A person not authorized to have access to specific classified information in accordance with the requirements of the NISPOM.

14. Abbreviations & Acronyms

AFSO	Assistant Facility Security Officer
AIS	Automated Information System
C	Confidential
CAGE	Commercial and Government Entity
COMSEC	Communication Security
CSA	Cognizant Security Agency
CSO	Cognizant Security Office
DoD	Department of Defense
DoD CAF	Department of Defense Central Adjudication Facility
DOE	Department of Energy
DSS	Defense Security Service
DTIC	Defense Technical Information Center
e-QIP	Electronic Questionnaires for Investigation Processing
FBI	Federal Bureau of Investigation
FCL	Facility (Security) Clearance
FSO	Facility Security Officer
GCA	Government Contracting Activity
GSA	General Services Administration
ISFD	Industrial Security Facilities Database
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ITAR	International Traffic in Arms
JPAS	Joint Personnel Adjudication System
KMP	Key Management Personnel
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NTK	Need-To-Know
OPM	Office of Personnel Management
PCL	Personnel Security Clearance
POC	Point of Contact
PR	Periodic Reinvestigation

<i>PSMO-I</i>	Personnel Security Management Office for Industry
<i>S</i>	Secret
<i>SCG</i>	Security Classification Guide
<i>SPP</i>	Standard Practice Procedures
<i>TS</i>	Top Secret
<i>U</i>	Unclassified
<i>US</i>	United States

15. References

- [1] National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M Change 2.