Insider Threat Program Policy

Version 3.0

January 1, 2019

NextStep Technology, Inc.
17485 Monterey Road, Suite 304
Morgan Hill, CA 95037

Table of Contents

Contents

Section 1 INTRODUCTION

An insider threat is the threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. 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 departmental resources or capabilities.

The National Industrial Security Program Operating Manual (NISPOM) paragraph 1-202, which provides baseline standards for the protection of classified information, requires contractors that engage with federal agencies, which process or access classified information, to establish an Insider Threat Program. The NISPOM requirement for an Insider Threat Program was preceded by Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. Signed by President Obama in September 2011, Executive Order 13587 requires federal agencies that operate or access classified computer networks to implement insider threat detection and prevention programs.

The program will gather, integrate, and report relevant and credible information covered by the 13 personnel security adjudicative guidelines that may be indicative of a potential or actual insider threat to deter all contractor employees granted personnel clearances (PCLs) and all employees being processed for PCLs, from becoming insider threats; detect any cleared person with authorized access to any government or contractor resources to include personnel, facilities, information, equipment, networks, or systems, who pose a risk to classified information; and mitigate the risk of an insider threat as defined above.

Section 2 SCOPE

This plan is specifically intended to educate NextStep Technology, Inc. (NEXTSTEP) employees about the requirements and standards to prevent, deter, detect, and mitigate actions by malicious insiders who represent a threat to national security or Department of Defense (DoD) personnel, facilities, operations, and resources. This plan establishes policy and assigns responsibilities for the Insider Threat Program (ITP). The ITP will seek to establish a secure operating environment for personnel, facilities, information, equipment, networks, or systems from insider threats.

NEXTSTEP has designated a corporate wide Insider Threat Program Senior Official (ITPSO), in writing, to establish and execute the insider threat program.

Section 3 APPLICABILITY

This Insider Threat Program Policy applies to all NEXTSTEP corporate offices, regions, and personnel with access to any government or contractor resources to include personnel, facilities, information, equipment, networks, or systems.

Section 4 RESPONSIBILITIES

4.1 Insider Threat Program Personnel and ITPSO

The ITPSO will be designated in writing and will act as the company's representative for ITP implementing activities. The designated ITPSO will be cleared in connection with the facility clearance, be a United States citizen, and will be designated as Key Management Personnel (KMP) in e-FCL in accordance with Cognizant Security Agency (CSA) guidance and in accordance with NISPOM 1-202b.

The ITPSO will be responsible for daily operations, management, and ensuring compliance with the minimum standards derived from Change 2 to DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)." Responsibilities include:

- Self-certify the Insider Threat Program Plan in writing to DSS no later than 6 months from the issue date of Change 2 to DoD 5220.22-M, NISPOM.
- Provide copies of the Insider Threat Plan upon request and will make the plan available to the DSS during the Security Vulnerability Assessments (SVA).
- Establish an Insider Threat Program based on the organization's size and operations.
- Provide Insider Threat training for Insider Threat Program personnel and awareness for cleared employees.
- Review user activity monitoring on classified information systems in order to detect activity indicative of insider threat behavior. These monitoring activities are 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 NISPOM 8-100d.
- Responsible for accessing, gathering, integrating, and reporting 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; detecting insiders who pose a risk to classified information; and mitigating the risk of an insider threat.
- Regularly meet with Human Resources to identify patterns of negligence or carelessness in handling classified information, in accordance with NISPOM 1-304c, even for incidents that do not warrant a culpability or incident report, and review any warnings or reprimands. Employee Performance Reviews will also be

periodically reviewed by the ITPSO to detect these patterns and, if necessary, a follow up with the immediate supervisor.

- Regularly conduct self-inspections of the Insider Threat Program that follow the established guidelines, in accordance with NISPOM 1-207b.
- The ITPSO will be notified immediately of any threat and oversee the collection, analysis, and reporting of information across the company to support the identification and assessment of insider threats by reviewing this documentation with the respective NEXTSTEP competencies, as warranted.
- Establish and manage all implementation and reporting requirements, to include self-assessments and independent assessments, the results of which shall be reported to the Senior Manager. These implementation and reporting requirements will be consistently reviewed and compared to new releases from DSS to maintain accordance with the most up-to-date version of the NISPOM.

Ensure that all NEXTSTEP employees are trained in:

- 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 (IS).
- Indicators of insider threat behavior, and procedures to report such behavior.
- Counterintelligence and security reporting requirements.

4.2 NEXTSTEP Employees

- Complete all required training in a timely manner.
- Report relevant and credible information coming to their attention. Such reporting includes information indicative of a potential or actual insider threat that is covered by any of the 13 personnel security adjudicative guidelines (see Section 5 under Adverse Information) or when that information constitutes adverse information, in accordance with paragraph 1-302a of the NISPOM.

Section 5 INDICATORS

5.1 Reportable Psychological/Behavioral Indicators

Insider threats are seldom impulsive acts. NEXTSTEP employees, former business partners and clients, wishing to harm NEXTSTEP's info structure, whether by stealing proprietary or government secrets or sabotaging information systems, usually plan their actions. Some wish to get revenge against the organization they believe wronged them. Others seek some kind of personal or financial gain, or to point out a perceived injustice. Still others may operate as spies for a foreign government. Regardless of their motivation, their plans often percolate for weeks, months, or even years before they act.

Building a baseline understanding of the personalities and behavioral norms of an insider threat will make detecting deviations in these norms easier. Some general behavioral characteristics of insiders at risk of becoming a threat include:

Characteristics of Insiders at Risk of Becoming a Threat	
Introversion	Minimizing their Mistakes or Faults
Greed/Financial Need	Inability to Assume Responsibility for their Actions
Vulnerability to Blackmail	Intolerance of Criticism
Compulsive and Destructive Behavior	Self-Perceived Value Exceeds Performance
Rebellious, Passive Aggressive	Lack of Empathy
Ethical "Flexibility"	Predisposition Towards Law Enforcement
Reduced Loyalty	Pattern of Frustration and Disappointment
Entitlement - Narcissism (Ego/Self-Image)	History of Managing Crises Ineffectively

Individuals that exhibit these characteristics may reach a point at which they carry out malicious activity against a company. One of the best prevention measures is to ensure NEXTSTEP employees recognize and report behavioral indicators exhibited by peers or business partners to your site FSO.

Some behavioral indicators of malicious threat activity:

- Remotely access the network while on vacation, sick or at odd times.
- Works odd hours without authorization.
- Attempts to bypass security controls.
- Request for clearance or higher level access without need.
- Notable enthusiasm for overtime, weekend or unusual work schedules.
- Unnecessarily copies material, especially if it is proprietary or classified.
- Interest in matters outside the scope of their duties.
- Chronic violation of organization policies.
- Decline in work performance.

- Irresponsible social media habits.
- Unexplained sudden affluence.
- Outward expression of conflicting loyalties.
- Unreported foreign contacts / foreign travel (when required).
- Maintains access to sensitive data after termination notice.
- Visible disgruntlement towards employer.
- Use of unauthorized digital external storage devices.
- Signs of vulnerability, such as drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health or hostile behavior, should trigger concern.
- Be on the lookout for warning signs among employees such as the acquisition of unexpected wealth, unusual foreign travel or unexpected absences.

5.2 Adverse Information

Adverse information consists of any information that negatively reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.

Examples of adverse information include culpability for security violations meeting the criteria of paragraph 1-304, NISPOM, use of illegal drugs, excessive use of alcohol, wage garnishments or other indications of financial instability, repeated instances of failing to follow established security procedures, the unauthorized release of classified information and/or unauthorized access to classified information systems, or other violations of information systems security requirements.

Such behavior raises doubts about an individual’s reliability, trustworthiness, and judgment in protecting national security.

These issues and concerns all relate to the 13 adjudicative guidelines:

1. Allegiance to the U.S.
2. Foreign Influence
3. Foreign Preference
4. Sexual Behavior
5. Personal Conduct
6. Financial Considerations

7. Alcohol Consumption
8. Drug Involvement
9. Psychological Conditions
10. Criminal Conduct
11. Handling Protected Information
12. Outside Activities
13. Use of Information Technology Systems

Reporting adverse information in a timely manner protects national security by allowing the DoD Consolidated Adjudications Facility to review and adjudicate issues as early as possible to determine whether an individual should remain eligible for access to classified information. Additionally, reporting adverse information can help employees receive the assistance they need, which might prevent a tragedy or harm to national security from occurring.

5.3 Documentation

Any incidents reported, verbal or nonverbal, shall be documented and be securely stored on file, regardless if it warrants a culpability or individual incident report. This process is to identify patterns of negligence or carelessness in handling classified information to ensure accurate reporting in accordance with the requirements outlined in paragraph 1-304 of the NISPOM.

Any consequences that result will be documented and follow NEXTSTEP's Three Step Disciplinary Action Policy and any other action deemed necessary by the supervisor, ITPSO and FSO, including termination of employment.

Section 6 INFORMATION SYSTEMS (IS) (Future)

At this time NextStep Technology, Inc does not have on-site information's systems – all IS work is conducted at the government or client facility.

In accordance with NISPOM paragraph 8-100d, a review of all IS audit records will be performed weekly by the ISSM or ISSO, if appointed. If analysis of the audit records reveals unauthorized actions that are not easily explainable or are indicative of an insider threat, the details will be reported to the ISSM and ITPSO for review and further action as necessary. Any incident that involves suspected compromise of classified information will be immediately reported to DSS through the appropriate channels. Below are guidelines and items to be aware of when reviewing automated audit records:

- Verify that the automated audit functions are performing properly and there are no time periods during which audit data is missing.
- Review all failed logins. Question multiple failed login attempts and account lockouts.

- Review a sampling of successful logins to ensure those persons were actually present and using their account during the recorded time periods. For example, if you are aware of someone being on travel or on vacation during the week, verify his or her account was not accessed.
- Question login sessions that occur at unusual times (e.g. 2 am) or sessions that are left open for long periods of time (i.e., over 24 hours).
- Scrutinize direct logins to generic or group accounts. Verify they are within the guidelines specified in the System Security Plan (SSP).
- If applicable, verify accesses to privileged group/generic accounts were made from authorized user IDs.
- Depending on the available audit mechanism, failed attempts to access objects may be all inclusive rather than limited to security-relevant objects. Attempt to focus your review on identifying any user ID that consistently has failed access attempts to privileged system files.

Section 7 REPORTING REQUIREMENTS

NEXTSTEP employees will report relevant information covered by the 13 personnel security adjudicative guidelines that may be indicative of a potential or actual insider threat to the site FSO and/or to the ITPSO. All credible insider threat information will be coordinated and shared with the ITPSO, which will then take action as directed in NISPOM, paragraph 1-300, "Reporting Requirements." The following information will be reported:

- 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, in accordance with NISPOM 1-302a, ISL 2006-02 and ISL 2011-4.
- Incidents that constitute suspicious contacts, in accordance with NISPOM 1-302b (Suspicious Contacts) and ISL 2006-02. Information coming to the ITPSO'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 NISPOM 1-301, and ISLs 2006-02 and 2013-05.
- Information determined to be any possible or potential successful penetration of a classified information system must be reported immediately to the CSA per NISPOM 1-401.

7.1 Reporting Procedures

If information is discovered that pertains to the 13 personnel security adjudicative guidelines that may be indicative of a potential/actual insider threat or detection of an insider who poses a risk to classified information, the ITPSO will access, gather,

integrate, and provide the relevant and credible information immediately to the necessary competencies, in accordance with NISPOM, paragraph 1-202b and 1-300. This will include, at a minimum, Human Resources, site FSO, IT Competency Lead/COO and immediate supervisor.

A formal meeting will then be scheduled to discuss any additional relevant information and resulting mitigation actions. Any formal action taken will be documented. If necessary, legal counsel will be consulted and will advise Senior Management on recommended legal mitigation and/or actions. This information will then be merged into a file that will be made available to DSS and reported accordingly.

7.2 Reports to be Submitted to the FBI

The FSO shall promptly submit a written report to the nearest field office of the FBI regarding information coming to the company's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations. An initial report may be made by phone, but it must be followed in writing, regardless of the disposition made of the report by the FBI. A copy of the written report shall be provided to the CSA.

7.3 Reports to be Submitted to the Cognizant Security Agency (CSA)

FSOs shall report adverse information coming to their attention concerning any of their cleared employees to the CSA. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. If the individual is employed on a Federal installation, NEXTSTEP shall furnish a copy of the report and its final disposition to the commander or head of the installation.

Section 8 REPORTING HOTLINES

Federal agencies maintain hotlines to provide an unconstrained avenue for government and contractor employees to report, without fear of reprisal, known or suspected instances of serious security irregularities and infractions concerning contracts, programs, or projects. NEXTSTEP has posted DSS required posters and provided this information in the employee brief. These hotlines do not supplant contractor responsibility to facilitate reporting and timely investigation of security matters concerning its operations or personnel, and contractor personnel are encouraged to furnish information through established company channels.

However, the hotline may be used as an alternate means to report this type of information when considered prudent or necessary. Contractors shall inform all employees that the hotlines may be used, if necessary, for reporting matters of national security significance. CSA hotline addresses and telephone numbers are as follows:

Defense Hotline
The Pentagon
Washington, DC 20301-1900
(800) 424-9098

U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program, MS 05 E13
11555 Rockville Pike
Rockville, MD 20852-2738
1-800-233-3497
TDD: 1-800-270-2787

DOE Hotline
Department of Energy
Office of the Inspector General
1000 Independence Avenue, S.W. Room SD-031
Washington, D.C. 20585
(202) 586-4073
(800) 541-1625

DNI Hotline
Director of National Intelligence
Office of the Inspector General
Washington, D.C. 20511
(703) 482-2650

Section 9 TRAINING

The NEXTSTEP designated ITPSO will ensure that NEXTSTEP program personnel assigned insider threat program responsibilities and all other employees, complete required training in accordance with paragraph 3-103 of the NISPOM. All new contractor personnel assigned duties related to the insider threat program management will complete the required training within 30 days of being assigned duties and refresher training annually thereafter. The new ITPSO will complete the required training within 30 days of being assigned ITPSO responsibilities.

NEXTSTEP insider threat program personnel, including the designated ITPSO, must be trained in:

- 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 legal, civil liberties, and privacy policies.

All cleared employees must satisfactorily complete insider threat awareness training prior to being granted access to classified information, and annually thereafter (NISPOM 3-103b). Insider Threat Awareness will be included in annual refresher training to reinforce and update cleared employees on the information provided in initial training in accordance with NISPOM 3-108. Training will address current and potential threats in the work and personal environment and will include at a minimum:

- The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the FSO.
- Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within ISs.
- Indicators of insider threat behavior, and procedures to report such behavior.
- Counterintelligence and security reporting requirements, as applicable.

The ITPSO and site FSO will establish and maintain a record of all cleared employees who have completed the initial and annual insider threat training.

Section 10 SECURITY REVIEWS AND INSPECTIONS

NEXTSTEP will review their program on a continuing basis and shall also conduct a formal self- inspection of the Insider Threat Program, including the self-inspection required by paragraph 1- 207b in the NISPOM, at intervals consistent with risk management principles.

These self-inspections will be related to the activity, information, information systems, and conditions of the overall insider threat program including sufficient scope, depth, and frequency; and management support in execution and remedy. The ITPSO will review self-inspections conducted at NEXTSTEP offices. NEXTSTEP will also prepare a formal report describing the self- inspection, its findings, and resolution of issues found then retain this report for CSA review through the next CSA inspection.

A NEXTSTEP senior management official and the ITPSO will certify to the CSA, in writing on an annual basis, that a self-inspection has been conducted, senior management has been briefed on the results, appropriate corrective action has been taken, and that management fully supports the insider threat security program.

Section 11 RECORDS MANAGEMENT

Insider Threat Training Records will consist of training attendance records, certificates, or other documentation verifying that personnel completed the training requirements in accordance with NISPOM 3-103c. The NEXTSTEP designated ITPSO will maintain records of all employee insider threat awareness, initial and refresher training. Insider Threat Training Records will be available for review during DSS security vulnerability assessments of all NEXTSTEP offices.

Section 12 GLOSSARY

Access: The ability and opportunity to obtain knowledge of classified information.

Adverse information: Any information that negatively reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.

Classified information: Information that has been determined pursuant to EO 13526, or any successor order, EO 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure and that is marked to indicate its classified status when in documentary form.

Cleared Contractor (CC): A person or facility operating under the National Industrial Security Program (NISP) that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level (and all lower levels).

Cleared Defense Contractor (CDC): A subset of contractors cleared under the NISP who have contracts with the Department of Defense. Therefore, not all cleared contractors have contracts with DoD.

Cleared Employee: A person who has been granted access to classified information, other than the President and Vice President, employed by, or detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

Compromise: An unauthorized disclosure of classified information.

Contact: Any form of meeting, association, or communication in person; by radio, telephone, letter, computer; or other means, regardless of who initiated the contact for social, official, private, or other reasons.

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 (EO 12333, as amended).

Departments and agencies: Refers to any ‘‘Executive agency,’’ as defined in 5 U.S.C.105; any ‘‘Military department’’ as defined in 5 U.S.C. 102; any “independent establishment,” as defined in 5 U.S.C. 104; and any other entity within the executive branch that comes into the possession of classified information.

Elicitation: The strategic use of conversation to subtly extract information about you, your work, and your colleagues.

Employee: For purposes of the National Insider Threat Policy, "employee" has the meaning provided in section 1.1(e) of EO 12968; specifically: a person, other than the President and Vice President, employed by, detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

Espionage: Defined under Sections 792-799, Chapter 37, title 18, United States Code (reference: Sections 792-799, Chapter 37 of title 18, United States Code) and Article 106a, Uniform Code of Military Justice (UCMJ) (reference: Section 801-940, Chapter 47, of title 10, United States Code, Uniform Code of Military Justice). Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies during war or peace. Reference (Sections 792-799, Chapter 37 of title 18, United States Code) makes it an offense to gather, with the requisite intent or belief, national defense information, by going on, entering, flying over, or obtaining access by any means to any installation or place used by the United States for national defense. The method of gathering that information is immaterial. Anyone who lawfully or unlawfully is entrusted with or otherwise has possession of, access to, or control over information about national defense, which he or she has reason to believe could be used against the United States or to the advantage of any foreign nation, and willfully communicates or transmits, or attempts to communicate or transmit, such information to any person not entitled to receive it may be punished under reference (Sections 792-799, Chapter 37 of title 18, United States Code). Anyone entrusted with or having lawful possession or control of information about national defense, who through gross negligence permits the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of that trust may be punished under reference (Sections 792-799, Chapter 37 of title 18, United States Code). If two or more persons conspire to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of reference (Sections 792-799, Chapter 37 of title 18, United States Code).

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

Insider Threat (IT): The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. 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 departmental resources or capabilities.

Insider Threat Program Senior Official (ITPSO): A designated U.S. citizen employee, who is a senior official and cleared in connection with the FCL, to establish and execute an insider threat program.

National Security: A collective term encompassing both national defense and foreign relations of the United States.

Sabotage: An act or acts with the intent to injure or interfere with, or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war materiel, premises or utilities to include human or natural resources, under reference (Sections 792-799, Chapter 37 of title 18, United States Code).

Security: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Subversion: An act or acts inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, of discipline, of the Military Forces of the United States.

Terrorism: The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Treason: Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason (see Section 2831 of title 18, U.S. Code, reference (Sections 792-799, Chapter 37 of title 18, United States Code).

Unauthorized Disclosure: A communication or physical transfer of classified information to an unauthorized recipient.

Unwitting: Inadvertent or accidental.