

U.S. National Industrial Security Program Security Incident Policy

Purpose

This policy establishes a Security Incident Program which includes a graduated scale of disciplinary actions. The purpose of the program is to enhance the protection of classified information, materials, equipment or areas by identifying, evaluating, and assigning responsibility for breaches of security associated with the aforementioned items. A graduated scale of disciplinary actions is required under section 1-304 of the National Industrial Security Program Operating Manual (NISPOM), DOD 5220.22-M, February 28, 2006, Chapter 1 (http://www.fas.org/sgp/library/nispom/5220_22m2.pdf), to which Mississippi State University agreed to abide by signing a security agreement, Form DD-441, (Attachment B) with the U.S. Department of Defense.

Policy

This policy applies to all personnel who possess a U.S. Government security clearance under Mississippi State University sponsorship.

Procedure

The significance of a security incident does not depend upon whether information was actually compromised. It depends upon the intentions and attitudes of the individual who committed the violation. Ability and willingness to follow the rules for protection of classified information is a prerequisite for maintaining a security clearance. Although accidental and infrequent infractions or minor violations are to be expected, deliberate or repeated failure to follow the rules is definitely not. It may be a symptom of underlying attitudes, emotional, or personality problems that are a serious security concern.

The following behaviors are of particular concern and may affect your security clearance:

- A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline.
- Taking classified information home, ostensibly to work on it at home, or carrying it while in a travel status without proper authorization.
- Prying into projects or activities for which the person does not have (or no longer has) a need to know. This includes requests for classified publications from reference libraries without a valid need to know, or any

attempt to gain unauthorized access to computer systems, information, or data bases.

- Intoxication while carrying classified materials or that causes one to speak inappropriately about classified matters or to unauthorized persons.
- Deliberate revelation of classified information to unauthorized persons to impress them with one's self-importance.
- Copying classified information in a manner designed to obscure classification markings. This may indicate intent to misuse classified information.
- Making unauthorized or excessive copies of classified material. Going to another office to copy classified material when copier equipment is available in one's own work area is a potential indicator of unauthorized copies being made.
- Failing to report requests for classified information from unauthorized individuals.

Definitions

A. Security Incident – a failure to safeguard classified documents, materials or items per applicable regulations. For MSU this is the National Industrial Security Program Operating Manual DOD 5220.2-M and Office of Research and Economic Development/Facility Security Office (ORED/FSO) policies.

B. Security Infraction – is a security incident that in the judgment of the ORED/FSO does not result in actual or possible compromise of the information. For example, at the end of the workday, an employee fails to record the closing of a security container or vault door on the SF-702 log sheet. Infractions are more administrative in nature, but are required to be documented to deter patterns of neglect or disregard for security procedures.

C. Security Violation – is a security incident that, in the judgment of ORED/FSO could result in the actual or possible compromise of the information. For example, not securing a security container or vault door at the end of the workday or when there are no cleared personnel present.

D. One year moving window – the period of time in which the aggregate of valid (as adjudicated by the ORED/FSO) security incidents will be counted. The period will start on the date of the most recent incident and extends backwards for a period of 12 months.

E. Collateral - A collateral security clearance is a clearance with no special access authorizations, e.g. SCI or SAP. Top Secret, Secret, and Confidential are collateral security clearances.

Security Inspections

The FSO, or her/his designee, is responsible for conducting security inspections of those facilities or areas that are utilized to store, process or work with classified information, materials or equipment. Inspections will be conducted on a routine basis; however, they can also be conducted on an unannounced basis depending upon the situation. A facility or area that is prone to security violations may be inspected on a more frequent basis.

Reporting & Adjudication of Security Incidents

All security incidents will be reported to ORED/FSO. Employees must inform the FSO orally or in writing of any improper security practice that comes to the employee's attention in order that remedial action may be taken. Reporting of security incidents is an honor system. All of us must take the responsibility upon ourselves to ensure that all classified items are secured properly and afforded all the protection required and when a security incident occurs initiate self-reporting.

Failure to report a security violation is itself a security violation and may be a very serious concern. After the arrest of Navy spy Jerry Whitworth, who was part of the infamous John Walker spy ring, interviews with Whitworth's work colleagues identified one who had noticed classified papers in Whitworth's personal locker, another who had observed Whitworth monitoring and copying a sensitive communications line without authorization, and a third who knew Whitworth took classified materials home with him but believed he was doing it only to keep his work current. Failure to report these violations enabled Whitworth's espionage to continue.

Upon the discovery or report of a security incident the ORED/FSO will open a file on the incident, start an investigation and initiate the ORED/FSO Record of Incident form (Attachment C).

The ORED/FSO, or her/his designee, will conduct an investigation of the reported security incident that will include, but not be limited to, personal interviews of person or persons involved, site visitation where the security incident occurred and the gathering of any additional information that pertains to the security incident investigation. All information will become part of the security incident file that will be kept in the ORED/FSO facility. The individual suspected of the incident will also be able to make a statement that is a part of the Record of Incident form.

The security incident will be adjudicated by the FSO utilizing only the information that is obtained from the incident investigation and that is documented. After the incident is adjudicated a final report will be written and forwarded along with all

investigative documentation to the Vice President for Research and Economic Development (V/P ORED) for review. After review and approval by the V/P ORED the individual(s) involved will be informed in writing of the findings.

All records associated with a security incident investigation will be kept in the office of the FSO. All records are open to those personnel directly involved in the security incident; however, they can not be removed or copied.

Appeal

An appeal to the validity or categorization of a security incident can be made in writing to the V/P ORED. The appeal must be received by V/P ORED within 7 days of receiving notification of the findings. The appeal will be based upon existing information; no new information can be introduced or considered in the appeal process.

Security Incident Examples

The following is not a complete list of infractions or violations but is a sampling of what could occur. The difference between an infraction and a violation can be very fine. Let's examine leaving classified material on your desk; in one instance you are in protected space, i.e. vaulted area with 24/7 alarm system; however, other personnel in the area may not have the same access as you even though they are cleared. The possibility of compromise is very low in this instance; consequently it can be viewed as an infraction. But consider the act of leaving classified material on your desk in an unsecured area; it is a violation because the possibility of compromise is very high. Both instances have the same scenario but two vastly different outcomes due to the security considerations affecting the situation.

Infractions:

- Failure to log opening or closing of a security container or vault door.
- As stated previously Infractions are more administrative in nature. You can be issued an infraction for leaving classified material out on your desk even if you are in a vaulted area that is approved for classified materials and there is a 24/7 monitored and approved alarm system which was operational and in use when the material was left out on the desk.

Violations:

- Leaving a classified file or security container unlocked and unattended either during or outside normal working hours.

- Keeping classified material in a desk or unauthorized cabinet, container, or area.
- Leaving classified material unsecured or unattended on desks, tables, cabinets, or elsewhere in an unsecured area, either during or after normal working hours.
- Losing classified material that has been entrusted to your care.
- Reproducing or transmitting classified material without proper authorization.
- Removing classified material from the work area in order to work on it at home.
- Granting a visitor, contractor, employee or any other person access to classified information without verifying both the individual's clearance level and need-to-know.
- Discussing classified information over the telephone or other than a phone approved for classified discussion.
- Discussing classified information in lobbies, cafeterias, corridors, or any other public area where the discussion might be overheard.
- Carrying safe combinations or computer passwords (identifiable as such) on one's person, writing them on calendar pads, keeping them in desk drawers, or otherwise failing to protect the security of a safe or computer.
- Failure to mark classified documents properly.
- Failure to follow appropriate procedures for the destruction of classified material.
- Tampering with a security container or vault door.

Disciplinary Actions

1. All personnel that have the responsibility to safeguard classified information/material from unauthorized access are subject to disciplinary actions (administrative and/or criminal).
2. Potential or actual infractions or violations of classified information/material must be reported immediately to the Facility Security Office to ensure the integrity of the information/material and the university. Failure to report or the misrepresentation of an infraction or violation is in itself a violation and may result in a disciplinary action. It is the responsibility of all personnel to act responsibly and to correct irresponsible or unauthorized behavior to prevent the compromise of classified information/material and to ensure the safety and security of other personnel, property and the university
3. The disciplinary action to be taken for a specific security infraction or violation will be decided upon by the VP/ORED and the FSO meeting together to discuss the infraction or violation. The disciplinary actions that may be taken are:

- Retraining
- Verbal warning
- Verbal reprimand
- Written reprimand
- Suspension of security clearance (see note 1 & 2)
- Termination of security clearance (see note 2)
- MSU HRM action
- Criminal actions

This guide does not dictate the disciplinary action to be taken; rather, it establishes a range of options that can be taken to ensure the safety and security of personnel and property. The action taken will be based upon the severity of each or subsequent infraction(s) or violation(s) and may include none, any, or all of the actions listed. Multiple infractions and/or violations within the one year period raise doubts about an individual's trustworthiness and ability to safeguard classified information /material.

4. All security incidents will become part of the individual's security record that is maintained by the FSO.

Notes:

1. Suspension of a security clearance can be for any length of time that is determined to be appropriate for the security incident and will be determined by VP/ORED and the FSO. Prior to the reinstatement of the security clearance a meeting to discuss the individual's suitability for a security clearance will be held. Attending will be the VP/ORED, the FSO, the individual and the individual's immediate supervisor. This meeting is mandatory for reinstatement of the security clearance.
2. Any clearance suspension or termination will be noted in the Department of Defense Joint Personnel Access System database. This is the database of record for the U.S. Government that tracks all industrial security clearances and actions.
3. Per NISPOM (DOD 5220.22-M) section 1-304 entitled "Individual Culpability Reports" any security violation that deliberately disregards security requirements, or, involves gross negligence in the handling of classified material, or, was not deliberate in nature but involves a pattern of negligence or carelessness will be reported to the Defense Security Service. Also the deliberate disclosure of classified information/material will also be reported to the FBI for criminal investigation.

Record of Incident Form

Attachment C is the record of what will be initiated when a security incident is discovered or reported. The FSO will fill out all areas of the form with the exception of section 2, which is the area for the statement of the person suspected of the incident. The completed form will become part of the security incident record.

Regulatory

Department of Defense Security Agreement, Form DD-441 (Attachment B)
National Industrial Security Program Operating Manual, DoD 5220.22-M, February 28, 2006 (Attachment A)
Classified Information Nondisclosure Agreement, SF-312 (Attachment D)

Review

The Vice President of Research and Economic Development and the Facility Security Officer are responsible for the review of this policy as needed but no less frequently than 4 years.

OP80.03
10/07/09

Recommended by:

/s/ Kirk Schulz
Kirk Schulz, Vice President for Research and Economic Development

Reviewed by:

/s/ Don Zant 04-22-09
Don Zant, Director of Internal Audit

/s/ Charles Guest 04-24-09
Charles Guest, General Counsel

Approved by:

/s/ Mark Keenum 10-07-09
Mark Keenum, President

Attachments: [A. National Industrial Program Operating Manual, Chapter 1](#)
[B. Department of Defense Security Agreement, Form DD-441](#)
[C. Security Incident Report Form](#)
[D. Classified Information Nondisclosure Agreement SF-312](#)