Standard Practice Procedures for Industrial Security

January 2023

Forward

The Curators of the University of Missouri (University of Missouri or UM) and selected subsidiaries maintain a Security Agreement with the Department of Defense in order to have access to information that has been classified because it would damage national security if improperly released.

The programs and activities at the University of Missouri and approved subsidiaries which require access to classified information are vital parts of the defense and security systems of the United States. All associated personnel are responsible for properly safeguarding the classified information to which they have been granted access.

This Standard Practice Procedures (SPP) conforms to the security requirements set forth in 32 CFR § 117[1], colloquially the National Industrial Security Program Operating Manual (NISPOM). This SPP provides cleared personnel with the requirements of the NISPOM as they relate to work performed across the University of Missouri System. This document should also serve as an easy reference when questions about security arise.

The University of Missouri fully supports the National Industrial Security Program (NISP)[2] and understands its obligation to implement security practices that contribute to the security of classified defense information.

Mun Y. Choi, President University of Missouri	5-17-22 Date

[1] https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117
[2] https://www.dcsa.mil/mc/ctp/nisp

Contents

I. Introduction

This Standard Practice Procedure (SPP) describes policies regarding the handling and protection of classified information. The SPP is applicable to all cleared employees, students, subcontractors, consultants, and visitors engaged in cleared contract projects and activities through any associated FCL to the University of Missouri System or its subsidiaries. In the event there is any discrepancy between the SPP and the National Industrial Security Program Operating Manual (NISPOM), the NISPOM shall take precedence.

II. Facili ty Information

A. Facility Clearance

A facility clearance (FCL) is an administrative determination that an entity is eligible for access to classified

D. Key Management Personnel

Key Management Personnel (KMPs) are those individuals having the authority and responsibility for planning, directing, and controlling a cleared facility. The Senior Management Official (SMO), who is the University of Missouri President, the FSO, and the Insider Threat Program Senior Official (see Section VII) are KMPs who must always be cleared to the level of each FCL. Other KMPs must either be cleared at the level of the FCL or excluded from classified access.

KMPs requiring a clearance are a designated member of the Board of Curators, and the Chancellor and Provost of every campus where personnel require a clearance to perform work on in furtherance of a classified contract. The remaining members of the Board of Curators, UM General Officers, and the Chancellor and Provost of any campus with no cleared personnel are excluded from access to classified information.

E. Insider Threat Program

The NISP also requires that UM establish and maintain an Insider Threat Program (ITP) that will gather, integrate, and report relevant and available information indicative of a potential or actual insider threat. The Insider Threat Program follows a corporate ITP structure. Information about the University of Missouri's Insider Threat Program is found in Section VII.

III. Personnel Security Clearances

A. Clearance Procedures

Personnel are processed for a personnel security clearance (PCL) only when a determination has been made that access to classified information is necessary for performance on a classified contract

E. Personal Changes

Cleared personnel must report personal changes as identified in SEAD 3 to the FSO through the reporting process and referencing the 13 Adjudicated Guidelines such as:

- Change in name
- Foreign travel not associated with cleared contract work
- Change in marital or cohabitation status
- Foreign contacts: continuing associations with foreign nationals that involve bonds of affection, personal obligation, or intimate contact
- Owning/trading foreign-backed assets, such as cryptocurrency
- Change in citizenship, voting in a foreign election, applying for/holding a foreign passport/ID card
- Access to classified information is no longer needed
- No longer wish to be processed for a personnel clearance or continue an existing clearance
- Termination of employment

Advance notification to the FSO is required if there is an intent to marry or cohabitate with a foreign national (including rooming situations).

F. Suspicious Contacts

The NISPOM defines suspicious contacts as:

- Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee
- Contacts by cleared employees with known or suspected intelligence officers from any country, or
- Contact which suggests a cleared employee may be the target of an attempted exploitation by the intelligence services of another country

Unsolicited requests for information are one of the most frequently reported collection methods. Emails which are obviously spam are not reportable. However, attempts that appear to be (1) specifically targeting UM or a subsidiary as a cleared contractor or targeting a DoD-related or protected technology, or (2) attempting to obtain classified, export-controlled, or proprietary information from UM personnel are valid suspicious contacts that require reporting.

VII. Insid er Threat Program

The University of Missouri and its subsidiaries utilize a corporate-

B. Insider Threat Program Senior Official

B. University of Missouri Ethics and Compliance Hotline

The University of Missouri established the "Integrity and Accountability Hotline" to provide employees with an anonymous avenue for reporting suspected incidences of ethics or compliance abuses. The reporting system is both web and telephone based and is available on a 24-hour/365-day basis for individuals to report known or suspected incidences of wrongdoing that compromise the University's operations and transactions. To access this confidential reporting hotline, call 1-866-447-9821 or go to https://secure.ethicspoint.com/domain/media/en/gui/40803/index.html?123.

X. Marking Classified Information

A. 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.

B. Original Classification

The determination to originally classify information occurs ONLY by a U.S. Government official who has delegated authority in writing. Classification occurs pursuant to Executive Order 13526 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.

C. Derivative Classification

Cleared personnel 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 IV regarding required derivative classification training.

XI. Safeguarding Classified Information

A. Information Management System

The University of Missouri has established an information management system (IMS) to protect and control the

Incoming classified materials for CAGE 9B964 must be sent to:

University of Missouri
Attn: Security Office
P.O. Box 1075
Columbia, MO 65205-1075

Incoming classified materials for CAGE 1DT80 must be sent to:

UMKC
Attn: Security Office
P.O

material stored; or when the person's clearance has been administratively terminated, suspended, or revoked

- The compromise or suspected compromise of a container or its combination, or the discovery of a container left unlocked or unattended

G. Retention of Classified Materials

FSOs will review classified holdings on a recurring basis for the purpose of maintaining classified inventories to the minimum required for classified operations. This review will take place at least annually during the self-inspections.

Classified materials may be retained for two years after the conclusion of the classified contract under which they were received. Before two years has passed, permission must be requested in writing to the GCA if additional retention is required. Contact the FSO for guidance.

H. Disposal of Classified Materials

The quantity of classified material on hand will be minimized to the smallest amount consistent with contractual performance. Once classified material has served its purpose, it will be returned to the government customer or destroyed by NISPOM directed methods as soon as possible. All destruction will be accomplished by authorized personnel and in the presence of a minimum of one witness.[13] Disposal of classified material will be recorded in the IMS. Contact the FSO for guidance.

I. End-of-Day Checks

The FSO, or a designated custodian assigned to an approved storage container, is responsible for ensuring that the container is locked and secured at the close of business each day. The end of day check will be recorded on the Security Container Check sheet (SF-702) located at every approved container. Additional end-of-day security checks, if needed, will be established through a project-specific amendment to this SPP.

J. Perimeter Controls

Perimeter controls have been established to deter and detect unauthorized introduction or removal of classified material. All persons who enter or exit locations with containers approved for the storage of classified information shall be subject to an inspection of their personal effects. All visitors and employees are subject to possible inspection, which will occur at random intervals.

K. Oral Discussions

Cleared personnel shall ensure that classified discussions will not take place over unsecure telephones, in public conveyances or places, or in any other manner that permits interceptio l d

Definitions

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.

Automated Information System (AIS) : A generic term applied to all electronic computing systems. Automated Information Systems (AIS) collect, store, process, create, disseminate, communicate, or control data or information. AIS are composed of computer hardware (e.g., automated data processing equipment and associated devices that may include communication equipment), firmware, an operating system (OS), and other applicable software.

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 Personnel : All University of Missouri personnel (including administrators, faculty, staff, students, and consultants) granted a personnel clearance or who are in process for a personnel clearance.

Compromise: An unauthorized disclosure of classified information.

Contractor : Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.

CONFIDENTIAL: Classified information or material that requires protection whereby unauthorized disclosure could reasonably be expected to cause damage to our national security.

Derivative Classification: Incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classification markings that applies to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Facility : A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operational entity.

Facility Security Clearance (FCL) : 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 National : Any person who is not a citizen or national of the United States.

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 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.

Key Management Personnel (KMP) : Senior management identified in a facility that require an eligibility determination in order for a facility to be granted a facility clearance.

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.

Original Classification : An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

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

Acronyms & Abbreviations

AIS	Automated Information System
C	Confidential
CSA	Cognizant Security Agency
DCSA	Defense Counterintelligence and Security Agency
DoD	Department of Defense
FCL	Facility (Security) Clearance
FSO	Facility Security Officer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ITP	Insider Threat Program
ITPSO	Insider Threat Program Senior Official
KMPs	Key Management Personnel
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
PCL	Personnel (Security) Clearance
PR	Periodic Reinvestigation
S	Secret
SCG	Security Classification Guide
SMO	

Research Security and Compliance

University of Missouri System

310 JesseHall
Columbia, Missouri 65211

www.umsystem.edu /research -security -and -compliance