



University of Missouri System

COLUMBIA | KANSAS CITY | ROLLA | ST. LOUIS

Standard Practice Procedures for Industrial Security

January 2023

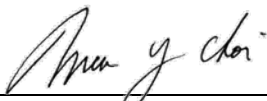
Forward

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 § 117¹, 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.....	4
II.	Facility Information	4
	A. Facility Clearance	4
	B. Storage Capability	4
	C. Facility Security Officer	4
	D. Key Management Personnel	5
	E. Insider Threat Program.....	5
III.	Personnel Security Clearances	5
	A. Clearance Procedures.....	5
	B. Reinvestigations	5
	C. Consultants	6
	D. Removal of Access.....	6
IV.	Security Education	6
	A. Initial Security Briefings.....	6
	B. Annual Security Briefings	6
	C. Derivative Classification Training	6
	D. Debriefings	7
V.	Security Vulnerability Assessments / Self Inspections	7
	A. Defense Counterintelligence and Security Agency.....	7
	B. Security Vulnerability Assessments (SVAs)	7
	C. Self-Inspections	7
VI.	Individual Reporting Responsibilities.....	7
	A. Espionage / Sabotage	8
	B. Adverse Information	8
	C. Loss, Compromise, or Suspected Compromise of Classified Information	8
	D. Security Violations	8
	E. Personal Changes	9
	F. Suspicious Contacts	9
VII.	Insider Threat Program	9
	A. Insider Threat Program Plan.....	9
	B. Insider Threat Program Senior Official.....	10
	C. Insider Threat Training	10
VIII.	Disciplinary Actions	10
IX.	Reporting Hotlines	10
	A. Department of Defense Hotline.....	10
	B. University of Missouri Ethics and Compliance Hotline	11

- X. Marking Classified Information..... 11
 - A. Classification Levels 11
 - B. Original Classification 11
 - C. Derivative Classification 11
- XI. Safeguarding Classified Information..... 11
 - A. Information Management System 11
 - B. Receiving Classified Materials 11
 - C. Transmission of Classified Information 12
 - D. Reproduction of Classified Materials 12
 - E. Storage of Classified Information..... 12
 - F. Combinations 12
 - G. Retention of Classified Materials 13
 - H. Disposal of Classified Materials 13
 - I. End-of-Day-Checks 13
 - J. Perimeter Controls..... 13
 - K. Oral Discussions 13
- XII. Public Release Disclosure 14
- XIII. Visit Procedures..... 14
 - A. Incoming Visits 14
 - B. Outgoing Visits 14
- XIV. Information System Security 14
- XV. Emergency Procedures..... 15
 - A. Emergency Plan 15
 - B. Emergency Contacts 15
- Definitions..... 16
- Acronyms & Abbreviations..... 18

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. Facility Information

A. Facility Clearance

A facility clearance (FCL) is an administrative determination that an entity is eligible for access to classified information or the award of a classified contract. The Defense Counterintelligence and Security Agency (DCSA), which is the Cognizant Security Agency (CSA) for the University of Missouri, makes the determination for any UM campus (considered subsidiaries) to receive a separate FCL to adequately safeguard or otherwise reduce the risk associated with accessing classified information.

As of 2022, UM is a “corporate family”³ with a “parent” and “subsidiary” FCL. As such, certain security functions required for 32 CFR §117 compliance are centralized and administered by UM. All FCLs associated with UM must comply fully with the NISPOM and all other requirements set forth below.

The UM FCL must be at the same or higher level than any individual campus. Identifying FCLs occur through the use of CAGE codes. The “parent” FCL is held by the Curators of the University of Missouri (UM) and is represented by CAGE 9B964. The subsidiary FCL is held by the University of Missouri-Kansas City (UMKC) and is represented by CAGE code 1DT80.

UM has a TOP SECRET (TS) facility clearance. The FCL is valid for access to classified information at the TOP SECRET or lower classification level.

UMKC has a SECRET facility clearance. The FCL is valid for access to classified information at the SECRET or lower classification level.

B. Storage Capability

The facility clearance level is separate from the storage capability level. Cleared contractors like UM must receive separate approval prior to storing any classified information. The University of Missouri and UMKC are approved to store classified material up to the SECRET (S) level. Section X discusses the procedures for appropriate handling, storage, and control of classified materials.

C. Facility Security Officer

Through the FCL process, each entity, the University of Missouri System and UMKC, agreed to adhere to the rules of the National Industrial Security Program (NISP). Under the NISP, both UM and UMKC appointed a Facility Security Officer (FSO). The FSO is a U.S. citizen, an employee, and cleared to the level of each FCL. The FSO must complete required training and is responsible for supervising and directing security measures necessary for implementing the NISPOM, related Federal requirements for classified information, and this SPP. Contact for Security staff for each FCL is provided to cleared personnel through various educational pieces.

³ 32 CFR 117.3(b) “Corporate family”

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

Each applicant for a security clearance must produce evidence of U.S. citizenship such as an original birth certificate, passport, or certificate of naturalization. Applicants must also provide the FSO with a hard copy set of fingerprints, which can usually be obtained through a local law enforcement agency such as those located on each UM campus.

Applicants will complete the Questionnaire for National Security Positions (SF-86). The FSO will ensure that prior to initiating the investigation request, the applicant is made aware in writing that the SF-86 is subject to review by the FSO only to determine that the information therein is adequate and complete but will be used for no other purpose at UM.

While it is the University of Missouri or its subsidiaries that initiate the clearance process for personnel, the U.S. government conducts the investigation and makes the determination of whether an individual is eligible to access classified information and grant the personnel clearance.

B. Reinvestigations

Cleared individuals are subject to a periodic reinvestigation (PR) at a prescribed period of time based upon their level of access. The FSO or other security staff is responsible for reviewing PCL records and ensuring personnel are submitted for PRs as required.

C. Consultants⁴

For security administration purposes, consultants are treated as employees of UM and must comply with this SPP and the NISPOM. Consultants with access to classified information will, however, be required to execute a Consultant Agreement which outlines their specific security responsibilities.

D. Removal of Access

The FSO may terminate an individual's PCL when access to classified information is no longer required or as requested per review of situations by the Insider Threat Working Group. In general, terminating a PCL when personnel no longer have "need-to-know" will not adversely affect an individual's eligibility to access classified information in the future. At the time a PCL is terminated, the individual will be debriefed (see Section IV).

IV. Security Education

A. Initial Security Briefings

All cleared personnel must receive an initial security briefing, complete insider threat awareness training (see Section VII), and sign a Nondisclosure Agreement (SF-312)⁵ prior to being granted access to classified material for the first time. At a minimum, the initial briefing will include the following:

- Threat Awareness Briefing
- Counterintelligence awareness
- Defensive Security Briefing
- Overview of Security Classification System
- Reporting Obligations
- Overview of the UM SPP

B. Annual Security Briefings

Annual briefings will be provided to all cleared personnel to reiterate their obligation to protect classified information and provide any updates to security requirements. Insider Threat Awareness training is also required annually for all UM cleared personnel (see Section VII). Training on Controlled Unclassified Information (CUI) is also required for cleared personnel requiring access to Department of Defense CUI. Additional training may be required or administered based on sponsor or contractual requirements.

C. Derivative Classification Training

Employees authorized to make derivative classification⁶ decisions must complete initial derivative classification training and refresher training at least once every two (2) years prior to making derivative classification decisions. Documentation identifying the date of the most recent training and type of training derivative classifiers receive is maintained. The FSO will provide guidance on how to access and complete the training.

⁴ If the University of Missouri or a subsidiary sponsors a consultant for a PCL, the consultant must be compensated directly for their work; otherwise, UM or its subsidiary must sponsor the company receiving compensation for a Faculty Security Clearance (FCL) and issue a subcontract to the company.

⁵ The SF-312 is an agreement between the United States Government and a cleared individual.

⁶ The process of determining whether information has already been originally classified and, if it has, ensuring that it continues to be identified as classified by marking or similar means when included in newly created material.

D. Debriefings

The FSO, or another member of the security staff, will debrief cleared personnel who no longer require a security clearance or terminate employment with UM or its subsidiaries.

V. Security Vulnerability Assessments / Self Inspections

A. Defense Counterintelligence and Security Agency

The Defense Counterintelligence and Security Agency (DCSA) is the government cognizant security agency (CSA) which provides oversight of cleared contractors' procedures and practices for safeguarding classified defense information. DCSA Industrial Security Representatives may contact personnel in connection with the conduct of a security vulnerability assessment, as part of an investigation of an unauthorized disclosure of classified information, or to provide advice and assistance on security related issues.

The DCSA field office for the University of Missouri and its subsidiaries is:

St. Louis Field Office - IOFNS
Defense Counterintelligence and Security Agency
303 Fountains Parkway, Suite 303
Fairview Heights, IL 62208

B. Security Vulnerability Assessments (SVAs)

The University of Missouri and its subsidiaries are individually assessed by DCSA on a periodic basis, generally not more than once every twelve months unless special circumstances exist. During a vulnerability assessment, DCSA Industrial Security Representatives will review security processes and procedures to ensure compliance with the NISPOM, and interview UM personnel as needed to assess the effectiveness of the security program. Cooperation with DCSA during the SVA is required of all cleared personnel and other administrators related to the classified research enterprise.

C. Self-Inspections

Security staff review the UM security program on an ongoing basis but also perform, on an annual basis, a formal self-inspection similar to the DCSA SVA. The purpose of the self-inspection is to assess each FCL's security procedures against NISPOM requirements to determine their effectiveness and identify any deficiencies/weaknesses. As part of this self-inspection, cleared personnel interviews can occur. The FSO must certify annually to DCSA that a self-inspection has been completed, the results have been provided to the SMO (UM President), and a plan has been implemented to address any findings.

VI. Individual Reporting Responsibilities

All cleared personnel must report any of the following information to the security staff based on SEAD 3⁷ and SEAD 4⁸ guidance. Self-reporting⁹ occurs through a centralized form, and security staff may follow up with the

⁷ See *Security Executive Agent Directive 3: Reporting requirements for Personnel*, available at <https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf>

⁸ See *Security Executive Agent Directive 4: National Security Adjudicative Guidelines*, available at <https://www.odni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf>

⁹ https://www.dcsa.mil/mc/pv/mbi/self_reporting/

individual to confirm reported information. Cleared personnel receive information about reporting depending on contractual obligations from sponsoring agency and eligibility level through various means. Security staff address any questions or concerns with cleared personnel as needed. Anonymous reports regarding a security concern about others can also go through the DoD Hotline or the UM Integrity and Accountability Hotline (see Section IX).

A. Espionage / Sabotage

Report any information concerning existing or threatened espionage, sabotage, or subversive activities. Security staff forwards a report to the FBI and DCSA.

B. Adverse Information¹⁰

Adverse information is any information regarding cleared personnel¹¹ which suggests that their ability to safeguard classified information may be impaired or that their access to classified information may not be in the interest of national security. Cleared personnel must report adverse information regarding themselves or another cleared individual to the FSO. Reports will be completed even if the employment ends or is terminated. Reportable adverse information includes:

- Relationships with any known saboteur, spy, traitor, anarchist
- Engaging in espionage or acting as an 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 of 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

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

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

D. Security Violations

Cleared personnel must report any failure to comply with a requirement of this SPP or of the NISPOM. See Section VII regarding disciplinary actions associated with security violations.

¹⁰ Reporting adverse information does not necessarily mean the termination of a personnel clearance. Reports should not be based on rumor or innuendo.

¹¹ Includes personnel in process for a clearance

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 cohabit 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. Insider Threat Program

The University of Missouri and its subsidiaries utilize a corporate-wide insider threat program. Therefore, UM self-certifies to DCSA that all obligations of an ITP have been met and reflect the most current NISPOM requirements for all CAGE codes: parent and subsidiaries.

A. Insider Threat Program Plan

The University of Missouri has developed a written corporate-wide Insider Threat Program Plan, signed by the President, describing:

- Capability to gather relevant insider threat information across functional areas (e.g., human resources, security, information assurance, legal)
- Procedures to (1) access, share, compile, identify, collaborate among functional elements, and report relevant information that may be indicative of a potential or actual insider threat; (2) deter cleared personnel from becoming insider threats; (3) detect insiders who pose a risk to classified information; and (4) to mitigate the risk of an insider threat

B. Insider Threat Program Senior Official

The University of Missouri ITP also requires that there be a designated an Insider Threat Program Senior Official (ITPSO). The ITPSO is a KMP who is cleared in connection with the FCL and is responsible for establishing and executing UM's Corporate-wide Insider Threat Program. Other personnel may form a working group to assist the ITPSO with their duties. The ITPSO can be reached at insiderthreat@umsystem.edu.

C. Insider Threat Training

Within thirty (30) days of being assigned duties related to Insider Threat Program Management, the ITPSO and working group personnel must complete training that addresses:

- 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 personnel must complete their insider threat awareness training before being granted access to classified information and annually thereafter. Training will include, at a minimum:

- 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 insiders and collect classified information
- Indicators of insider threat behavior and procedures to report such behavior
- Counterintelligence and security reporting requirements, as applicable

VIII. Disciplinary Actions

Disciplinary action taken by the University of Missouri, or its subsidiaries is based upon a review of each case's own merits. The seriousness of the violation will be determined by whether a compromise, suspected compromise, or loss of classified information has occurred, or if it was only administrative in nature. Disciplinary action may be any one or more of the following depending upon the above factors: counseling and verbal warning, additional training, a written reprimand, revocation of security clearance, dismissal from the University or its subsidiary, or even criminal filing.

IX. Reporting Hotlines

Personnel at the University of Missouri or one of its subsidiaries may also make any mandatory reports (see Section VI) to the below hotlines in lieu of, or in addition to, reporting directly to the FSO. Reports to these hotlines can be made anonymously and without fear of reprisal.

A. Department of 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.

Hotline Phone Number: 800-424-9098 / 703-604-8799

Hotline Fax: 703-604-8567

To report online: <http://www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/>

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 classified information located/stored at UM. Any classified information generated at, or received by, the University of Missouri is logged into the IMS.

B. Receiving Classified Materials

All incoming classified material will be received by approved security staff (e.g., FSO or AFSO). The FSO will check all materials for evidence of tampering and the contents will be checked against the accompanying receipt. Incoming classified material will be logged into the IMS

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. Box 45120
Kansas City, MO 64171-8120

C. Transmission of Classified Information

When it becomes necessary for classified material to be sent to another location, contact the FSO for assistance. Only approved methods of transmitting classified information will be used. All outgoing transmissions will be accompanied with a receipt identifying the sender, addressee, and document for the recipient to sign and return. Transmissions will be logged into the IMS; the IMS will also be used to verify the signed receipt has been returned to the originating location.

D. Reproduction of Classified Materials

Classified information may only be reproduced on approved copy machines. Any new classified material that is generated via reproduction must be logged into the IMS. Contact the FSO for assistance.

E. Storage of Classified Information¹²

The University of Missouri and its subsidiaries are currently approved to store classified material up to the SECRET level. Each FSO maintains a list of locations and storage containers approved for classified storage. The following procedures apply:

- Only approved containers meeting NISPOM standards may be used to store classified information
- Containers must be locked when not under direct supervision of an authorized individual
- All classified material must be secured in the appropriate security container at the end of each working day

F. Combinations

Only a minimum number of authorized individuals will have knowledge of the combinations for security containers where classified material is stored. The Security Office maintains a record of individuals with access to each container. Authorized persons should memorize the combinations of classified security containers. If a written record of the combination is made, it will be marked and safeguarded in accordance with the highest level of material stored in the container.

Combinations will be changed by a person authorized access to the contents of the container or by the FSO as soon as possible following:

- The initial receipt of an approved container or lock
- The reassignment, transfer, or termination of any person having knowledge of the combination; when the security clearance granted to any such person is downgraded to a level lower than the category of

¹² Classified information cannot be removed from UM approved storage containers for use or storage at an individual's private residence.

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 interception by unauthorized persons. It is the responsibility of the person disclosing classified information to determine the need-to-know and eligibility of the receiving party(ies). Personnel who need to have a classified discussion should contact the FSO for additional assistance.

¹³ For destruction of TOP SECRET material, two witnesses are required. For destruction of SECRET and CONFIDENTIAL material, one witness is required.

XII. Public Release Disclosure¹⁴

In general, UM and cleared personnel are restricted from disclosing classified or unclassified information pertaining to a classified contract to the public without prior review and approval by the government customer. If cleared personnel would like to make a presentation, publish research results or other information, create brochures, reports, or similar materials, etc. on subject matter related to a classified contract, even if comprised solely of unclassified information,¹⁵ the FSO or a designated security staff member determines if prior approval must be obtained from the government customer (sponsor).

The following information typically does not need to be submitted for approval to release unless specifically prohibited by the GCA:

- The fact that a contract has been received, including the subject matter of the contract and/or type of item in general terms provided the name or description of the subject matter is not classified
- The method or type of contract, such as, bid, negotiated, or letter
- Total dollar amount of the contract unless that information equates to (a) a level of effort in a sensitive research area, or (b) quantities of stocks of certain weapons and equipment that are classified
- Whether the contract will require the hiring or termination of employees

XIII. Visit Procedures

A. Incoming Visits

All incoming classified visits are requested and approved through Security staff verifies each visitor's security status prior to allowing classified access through the system of record. The responsibility for determining need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit. Prior to the disclosure of classified information to a visitor, positive identification of the person must be made.

B. Outgoing Visits

All classified visits require advance notification to, and approval of, the place being visited. When cleared personnel need to visit other cleared contractors or Government agencies and access to classified information is anticipated, employees must notify security staff and provide relevant information for the visit to be submitted in the system of record. Ample time must be allowed to permit the visit authorization request to be prepared, submitted to the contractor/agency, and processed by their visitor control.

XIV. Information System Security

Processing of classified materials on an Automated Information Systems (AIS) requires prior approval/accreditation from DCSA and can only be established when processing is required in fulfillment of a classified contract. An accredited AIS will be classified no higher than the level of safeguarding for which safeguarding is approved. The Information Systems Security Manager (ISSM) will maintain System Security Plans (SSP) for all classified information systems.

¹⁴ Classified information made public is not automatically considered unclassified. Cleared personnel shall continue the classification until formally advised to the contrary. Personnel should report any information they believe to be classified that is in the public domain to the FSO.

¹⁵ Information that has been declassified is not automatically authorized for public disclosure.

Classified information CANNOT be entered into any computer or other electronic device at any location if it has not been formally approved/accredited for classified processing. Approved/accredited information systems, computers, or other devices will be clearly marked as such. If you have any question as to whether a system is approved, please contact the FSO or ISSM.

XV. Emergency Procedures

A. Emergency Plan

In emergency situations (fire, medical emergency, power outage, etc.), it is important to safeguard all classified information as best as possible. However, the overriding consideration in any emergency situation is the safety of personnel. Lives should not be endangered in order to secure classified information. Evacuate immediately if necessary and call the appropriate response/emergency unit. If time and conditions permit, return all classified materials to the storage container, and then secure the container. Seek out security staff for further instructions once in a safe environment.

B. Emergency Contacts

In the event that the FSO is not available, and an urgent or hazardous situation must be reported, personnel should contact their campus and/or municipal police department by calling 911 or using a non-emergency phone number.

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 with the requirements of the NISPOM.

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	Senior Management Official
SPP	Standard Practice Procedures
SSP	System Security Plan
TS	Top Secret
U	Unclassified
US	United States



University of Missouri System



Research Security and Compliance

University of Missouri System

310 Jesse Hall
Columbia, Missouri 65211

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