430.010 Industrial Security Program

Bd. Min. 6-27-24; Amended Bd. Min. 11-20-24

A. **Statement of Purpose**

1. This rule addresses The Curators of the University of Missouri (a.k.a., the University of Missouri System (UM System)) compliance with U.S. industrial security policy, including applicable federal statutes, Executive Orders (E.O.), Code of Federal Regulations (CFR), Department of Defense Instructions (DoDI), and other applicable authorities. UM System is committed to compliance for the protection of classified information disclosed to or developed by contractors of the U.S. Government (USG), employed or the responsibility of UM System (contractors).
2. This rule will be applied to achieve compliance with applicable federal authorities, including:

    a) E.O. 12829, National Industrial Security Program
    b) E.O. 10865, Safeguarding Classified Information within Industry
    c) 32 CFR Part 2004, National Industrial Security Program
    d) DoDI 5220.22, National Industrial Security Program
    e) 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM)

3. This rule implements policy, assigns responsibilities, and establishes requirements for the protection of classified information disclosed to, or developed by contractors across the UM System.

B. **Scope and Compliance Policy**

1. This rule applies to all cleared facilities (i.e., Facility Clearances or FCLs) within the UM System holding a FCL, to all personnel whose personnel security clearances are held by a UM System or subsidiary FCL, and to all personnel who hold roles related to ensuring compliance with the authorities outlined in subsection A.2 (e.g., Key Management Personnel or KMPs).
2. The UM System is the "corporate family" for all classified work taking place at any FCL within the System. Individual universities may have subsidiary Facility Clearances under the UM System Facility Clearance if they have federal authorization to hold classified materials on-site, a secondary place-of-performance, or flow down to a sub-tier contractor.
3. The UM System shall implement a corporate-wide Insider Threat Program to address insider threats throughout the UM System.
4. The President will appoint the following personnel to oversee and implement the UM System industrial security program (ISP) (System ISP):

    a) Senior Management Official (SMO)
    b) Insider Threat Program Senior Management Official (ITPSO)
    c) Facility Security Officer (FSO)

5. The personnel identified in subsection B.4 must:

    a) Oversee the implementation of the requirements of the NISPOM;

b) Undergo the same security training that is required of all contractors, in addition to any position specific training;
c) Be designated in writing; and
d) Undergo a personnel security investigation and national security eligibility determination for access to classified information at the level of the entity's eligibility determination for access to classified information.

6. SMO: The President of the UM System is the SMO for the UM System FCL and for all subsidiary FCLs held by an individual university within the UM System. The SMO will:

    a) Ensure a system of security controls in accordance with the NISPOM;
    b) Appoint an UM System ITPSO and FSO in writing;
    c) Remain fully informed of the UM System ISP classified operations;
    d) Make decisions based on the threat reporting and information and the potential impacts to the UM System ISP; and
    e) Retain accountability for the management and operations of the System's ISP without delegating that accountability.

7. ITPSO: The Director, Research Security and Compliance is the ITPSO and will be designated in writing by the SMO. The ITPSO will:

    a) Ensure the FSO(s) is part of the insider threat program;
    b) Complete training in accordance with the NISPOM; and
    c) Develop an insider threat program that meets the requirements of the NISPOM.

8. FSO: An FSO will be appointed in writing by the SMO for any University with an active FCL. Each FSO will:

    a) Supervise and direct security measures necessary for implementing the NISPOM to ensure the protection of classified information.
    b) Complete security training as deemed appropriate by the Cognizant Security Agency (CSA) who accredits the FCL. Both direct and reciprocity CSAs training must be met.
    c) Appoint an Information System Security Manager (ISSM) if classified information will be processed on an information system at a University with an FCL.

9. ISSM: If classified information will be processed on an information system at a University with an FCL, the FSO will appoint an ISSM. Each ISSM will:

    a) Be adequately trained and possess the technical competence required to operate, maintain, and secure the contractor's classified information system; and
    b) Oversee development, implementation, and evaluation of the University's classified information system program.

C. **University of Missouri Research Security and Compliance Team**

1. UM Research Security and Compliance Team
   Each FCL within the UM System will have an appointed FSO who reports to the UM System Director of Research Security and Compliance. Each FSO shall be a member of the University of Missouri Research Security and Compliance Team ("UM RSC Team").
2. Collaboration
   Recognizing both the necessity and administrative efficiencies gained, the UM RSC Team shall work in collaboration with each other and with those also holding

responsibilities for compliance with the authorities outlined in subsection A.2. to ensure that no single point of failure exists within the System.

3. Accountability and Alignment
   To ensure the accountability and alignment of the UM RSC Team, each Chancellor shall designate one of that University's Vice Chancellors to work with the UM System Director for Research Security and Compliance, who will jointly approve the following as it relates to the FSO at each institution:

   a) Recruitment and hiring decisions;
   b) Disciplinary and termination decisions; and,
   c) Annual performance evaluations and compensation decisions.

   For situations in which concurrence is not reached, the collective decision will be made with the President.

D. **Strategies**

1. The FSO(s) will develop the industrial security strategies for the UM System to establish, document, and implement processes and procedures to ensure the System remains in compliance with the authorities outlined in subsection A.2. These strategies will be brought before the UM RSC Team for approval before implementation.
2. A Standard Practice Procedures (SPP) is developed and maintained by the UM RSC Team. This SPP documents the current processes and procedures used across the System. The SPP will contain information describing acceptable structures for the Security Executive Committee (SEC).
3. University-specific appendices will be maintained within the SPP as needed.
4. At least once annually, the Board of Curators will review and ratify a Security Resolution outlining the members of the SEC and those who are excluded from the SEC in alignment with the structure outlined in the SPP.

E. **Implementation**

The FSOs and Insider Threat Program Senior Official on the UM RSC Team are responsible for the implementation of the industrial security programs and the Insider Threat Program for the UM System.