

## APPENDIX B

### State of Montana Security Roles and Responsibilities

Pursuant to 2-15-114, MCA, Security Responsibilities of Departments for Data, each department head is required to designate an information security manager to administer the department's security program. This position, along with others within the organization, performs duties associated with a strong security program. This document contains these roles and identifies responsibilities associated with them in regards to information security as well as provides a recommended reporting structure.

#### ROLES AND RESPONSIBILITIES

The following roles and responsibilities are recommended as key positions to an adequate information security program according to NIST guidance. Not all of these positions may be applicable depending on the size and scope of the organization. A primary consideration should be how to combine responsibilities in smaller organizations or when manpower is limited where separation of duties and conflicts of interest can still be maintained for the intent and needs of security. Some of the roles explained below are grouped and in some larger organizations these may have two or more individuals or levels of management assigned to these roles with more specific responsibilities. This list is a good representation of the main groupings of functional security roles to provide a well-rounded information security program and should apply to most state agencies.

- A. Senior Management. The department head will ensure that an information security program is implemented and sustained sufficient to support the mission of this organization. Recommended responsibilities:
  - Approves system security plans,
  - Approves security assessment plans/reports,
  - Approves memorandums of agreement or understanding,
  - Approves plans of action and milestones,
  - Authorizes operation of an information system,
  - Issues an interim authorization to operate the information system under specific terms and conditions,
  - Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist, and
  - Oversees the budget.
- B. Security Management. The Department Head will appoint an Information Security Manager (ISM) who directs the organization's day-to-day management of the organizations information security management program to include coordination of all security-related interactions both internal and external while maintaining a documented program (integration with continuity and records management). This position fulfills the requirements of 2-15-114, MCA. Recommended responsibilities:

- Designates an Information Security Officer (ISO) who shall carry out the ISM's responsibilities for system security,
- Ensures information security policies and procedures are developed and maintained,
- Ensures the identification, implementation, and assessment of common security controls,
- Ensures that personnel with significant responsibilities for system security plans are trained,
- Ensures adequate system security planning for department,
- Ensures that an organization-wide information security program is effectively implemented,
- Ensures information security considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, and acquisition/system development life cycles,
- Ensures information systems are covered by an approved security plan and are authorized to operate by the Agency Authorizing Official , and
- Ensures there is centralized reporting of all security-related activities.

Information Security Officer. The Information Security Officer (also known as the Information Systems Security Officer) may be the same individual designated by the agency head to administer the agency's security program for data under §MCA 2-15-114. Responsible for helping to ensure that the appropriate operational security posture is maintained for each information system as well as the overall operational requirements of the technology platform. Specific responsibilities are:

- Evaluating real or suspected IS security incidents within the agency and all component organizations;
- Providing resolution recommendations to the agency head, any attached agencies and division administrators; and
- Developing agency policies, standards, and procedures in evaluating and referring the investigation to other qualified entities, including law enforcement.

Recommended responsibilities:

- Carries out the IIM's responsibilities for system security planning,
- Coordinates the development, review and acceptance of system security plans with Information System Owners, Operational Information System Security Officer(s), Information System Security Developers, and the CIO,
- Coordinates the identification, implementation, and assessment of the common security controls,
- Serves with the Applications Manager as the ISM's primary liaison to the Information System Owners, maintains information security duties as a primary responsibility,
- Identifies, implements, and assesses the common security controls, and
- In partnership with the Applications Manager, coordinates with the Information System Owner any changes to the system and assesses the security impact of those changes.

C. Program and Functional Managers/Application Owners. Responsible for a program or business function (e.g., procurement or payroll) including the supporting computer system(s). Their responsibilities include providing for appropriate security, including management, operational, and technical controls. These officials are (*usually assisted*) supported by a technical staff that oversees the actual workings of the system with mid-level management helping develop and implement security requirements.

Recommended responsibilities:

- Develops the system security plan in coordination with assigned Information

Commented [JPF1]: STD-Computer Security Incident Management

System Security Developers, Operational Information System Security Officer(s), and functional "end users,"

- Maintains the system security plan,
  - Ensures that the system is deployed and operated according to the agreed-upon security requirements,
  - Ensures that system users and support personnel receive the requisite security training,
  - Updates the system security plan whenever a significant change occurs,
  - Assists in the identification, implementation, and assessment of the common security controls of both the application and the information,
  - Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior),
  - Shares information regarding the security requirements and security controls for the information where the information resides, and
  - Decides who has access to the information system and with what types of privileges or access rights, and
- D. Technology Providers/System Management/System Administrators. These personnel are the managers and technicians who design and operate computer systems. They are responsible for implementing technical security on computer systems and for being familiar with security technology that relates to their system(s); ensuring consistent confidentiality, integrity, and availability. Recommended responsibilities:
- Plays an active role in the continuous monitoring of critical systems and the overall environment,
  - Act as a consultant to the Information System Owner to ensure thorough security plans exist,
  - Manages and controls changes to the system and assess the security impact of those changes
  - Develops secure back-up and restore functions, and
  - Executes the commands necessary to provide the access to the information systems as defined by the Information System Owner.
- E. Supporting Functions. The security responsibilities of managers, technology providers and security officers are supported by functions normally assigned to others. Some of the more important of these may be Auditors, Physical Security, Disaster Recovery/Contingency Planning, Quality Assurance, Procurement, Training, Personnel (HR), Risk Management/Planning Staff, and the Physical plant or office (General Services Division).
- F. Department Users. Regardless of the direct or indirect interaction with computers or other information systems and processes the users and the functional managers/application owners (or their representatives) are responsible for identifying and making known the needs and requirements for protection of information; confidentiality, integrity and availability. Department employees play a critical role for information security in complying with established procedures and providing the front line defense and prevention of potential breach and reduced risk.
- G. Contract Users. Any contracted vendor who interacts with State or Department information systems (computer supported or hardcopy) must support and comply with all established security protocols and requirements.
- H. State Customers. This Department will monitor and interact with State customers and e-Gov users who access public information and other State web and internet resources to ensure continuity with confidentiality, integrity, and availability of information on all

State Systems.

- I. Security Teams/Councils/Working Groups. The Department will participate with established security teams (Councils/Working Groups) which directly support best practice initiatives for continuous improvement and continuity of Department and State-wide missions.

## REPORTING STRUCTURE

It is recommended that the Information Security Manager (ISM) report directly to the Director or Agency Head. This reporting structure is recommended because of the necessity of the ISM to be able to perform effectively and independently.

## SKILLS AND ABILITIES

Successful ISMs must have a broad range of business management and technical security skills. Possessing a background in the development and subsequent enforcement of security policies and procedures, security awareness programs, business continuity and disaster recovery plans, IT, auditing, and applicable industry and governmental compliance issues is critical. They must be savvy in understanding the business needs of an agency and be fully supportive of its mission and goals. Some areas where an ISM must possess adequate skills and abilities include:

- **Strategic** - An agency ISM must understand the agency's program areas and business needs and their role within the activities of the agency. The ISM must keep abreast of evolving technologies to ensure appropriate security controls are implemented and maintained as agency processes change. Identifying security risks to the agency and being able to evaluate and recommend appropriate security measures, from a strategic perspective, will help management understand the risks and the need to reduce them to acceptable levels.
- **Management and Communication Skills** – The ability to effectively communicate, both verbally and in writing, across all levels of management and the user community cannot be understated. The need to interact with critical staff (such as executive management, the Privacy Officer, the CIO, and the disaster recovery coordinator) and other agency business units (such as the legal, human resources, IT, procurement, business services, facilities management offices) to cooperatively achieve the goals is critical to the success of the information security program. The ability to write effectively, to explain information security in layperson terms, can be difficult. Executive management may not understand why a certain security component costs so much, or why it is important to the agency's goals. Possessing the ability to effectively develop issue papers, memorandums, letters, work plans, and other types of written communication can be invaluable in documenting security concerns and decisions, and in explaining important perspectives.
- **Technical Competence** – ISMs are required to have a certain level of technical competence to lead their organization's security initiatives. They need a general knowledge of how technical issues affect the business of the agency. It is very difficult for a security leader to be respected by their agency, regardless of size, without having a proper grasp of the technical security issues that affect it. Further, it would be difficult to

garner the respect of the other technical staff within the organization without that knowledge.

Being passionate about information security is critical to the success of the program. If an ISM is not fervent about it, he or she may find that is not the right career choice for them. Those ISMs that are fanatical about it should recognize that there is sometimes a fine line between passionate and obsessive. An important function of the ISM is to not always to say, "NO!" but to find secure ways to implement technologies while carefully weighing the risks against the business needs of the agency.

DRAFT - 2015