Enterprise IT Security Incident Response Policy

Subject: Information Technology

Revised: November 7, 2012

Effective: November 7, 2012

Review Date: November 2015

Responsible Party: Enterprise Chief Information Officer

- TABLE OF CONTENTS

100.00 Introduction

This policy governs the general response to and handling of computer and information security incidents. The policy establishes responsibility and accountability for addressing suspected computer security incidents and investigations.

200.00 Policy

200.10 Board of Regents policies governing the use of university information technology apply to all University faculty, staff, students, and patrons. All users of University information technology must comply with MSU Enterprise policies as well as Board of Regents policies, state and federal law. References to associated policies and laws are provided in section 400.00.

200.20 When a suspected security incident or request for investigation involving the MSU computing, networking, or information environment is identified, the procedures outlined in the Incident Response Guidelines for each campus shall be followed.

200.30 The Incident Response Management Team is responsible for management decisions related to incident handling. Decisions include, but are not limited to, the extent to which forensics will or will not be performed, the need to include additional entities in the response (Legal Counsel, University Police, external agencies, etc), and any communication and notification activities.

Incident Response Management Team members include for each campus:

Response Team Type	MSU-Billings	MSU-Bozeman	Great Falls College MSU	MSU-Northern
Incident Response Management Team	Chief Information Officer Associate Chief Information Officer Director of University & Government Relations (as needed) Unit Directors or Department Heads (as needed)	Enterprise Chief Security Officer Enterprise Chief Information Officer Director, Communications and Public Affairs (as needed) Unit Directors or Department Heads (as needed)	Chief Technology Officer Bozeman Chief Security Officer Executive Director Community Relations (as needed) Unit Directors or Department Heads (as needed)	Chief Information Officer Bozeman Chief Security Officer Executive Director Community Relations (as needed) Unit Directors or Department Heads (as needed)

200.40 The Incident Response Operational Team is responsible for hands-on response activities. This includes identifying the type of incident (physical theft, worm infection, server breach, inadvertent posting, etc), determination of the type of data involved and extent of exposure (when applicable), whether or not the breach is still active, and all other appropriate response and remediation steps as authorized and directed by the Incident Response Management Team in accordance with the Incident Response Guidelines.

Incident Response Operational Team members include for each campus:

Response Team Type	MSU-Billings	MSU-Bozeman	Great Falls College MSU	MSU-Northern
Incident Response Operational Team	Chief Information Officer Associate Chief Information Officer Operational Security Staff & Desktop Support as appropriate Others as appropriate representing data	Representatives from the MSU Security Committee Representatives from the MSU Security Operations Team Others as appropriate	Representatives from MSUGF IT Services Representatives from MSU Security Operations Team Others as appropriate	Representatives from MSUN IT Services Representatives from MSU Security Operations Team Others as appropriate

owners and
management

200.50 If the incident is deemed to be the result of intentional or negligent violation of MSU Policy, sanctions may be levied which may include departmental responsibility for the cost incurred responding to the incident, mandatory training for departmental personnel, and/or other steps as deemed appropriate by the IT Governance Council.

200.60 If public notification is required as a result of the incident, the division leader is the responsible party for notifying and managing communications in conjunction with the Incident Response Management Team.

200.70 Ultimate authority to interpret this policy rests with the President but is generally delegated to University Chief Information Officers and University Legal Counsel in conjunction with the Enterprise Chief Security Officer.

300.00 Procedures

Individual campuses maintain campus-specific standards and procedures that implement this policy. Campus-specific standards and procedures are currently under development; when published, the links to those pages will be provided here. Constituents will be required to comply with any standards and procedures developed for their campus:

- MSU-Billings
- MSU-Bozeman*
- Great Falls College MSU
- MSU-Northern

** MSU agencies follow MSU-Bozeman campus procedures*

400.00 References

No specific references exist for this policy.

500.00 Definitions

"Constituent" refers to any individual or group who has a stake in the University including students, staff, faculty, or patrons as well as any contractors, regents, committees, councils, groups, agencies, departments, entities, campus, or community.

"Enterprise" refers to all Universities, colleges, and agencies of Montana State University.

"Enterprise Chief Information Officer" refers to the top level information technology leadership role based on the Bozeman campus whose responsibilities include information technology leadership of the four MSU campuses.

"Enterprise Chief Security Officer" refers to the University's top-level IT security position based at MSU-Bozeman.

“Information Technology” or “IT” refers to any resource related to the access and use of digitized information, including but not limited to hardware, software, devices, appliances, network bandwidth and resources.

“Security Incident” refers to theft, loss, misuse, exposure, or other activities contrary to the Data Stewardship policy; intrusion, denial of service, corruption of software; or other breach or compromise of the University’s information infrastructure resulting in an impact to University operations.

“Security Investigation” refers to monitoring, copying, or facilitating access for authorized individuals to any computing or information resource as part of a personnel, legal, or criminal investigation.

“University” refers to any and all campuses, agencies, departments, or entities within the Montana State University enterprise.

“University Chief Information Officers” refer to the top-level IT position at each campus.

“University Legal Counsel” refers to the University’s attorney and/or designated legal staff based at MSU-Bozeman.