Salisbury University

Cybersecurity Incident Response Policy

1. PURPOSE

The Salisbury University Information Technology (SUIT) department is committed to managing the confidentiality, integrity, and availability of information technology assets and information. This includes providing timely, efficient, and effective response to cybersecurity incidents.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication

3. SCOPE

This policy is applicable to all SUIT environments and assets utilized by the University. SUIT will be responsible for ensuring the incident management plan is aligned with the requirements in this policy.

4. BASE POLICY AND COMPLIANCE REFERENCES

SUIT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other organizations. This policy serves as SU's authoritative adaptation of these policies with specific amendments to meet the business and operational needs of the University.

Policy References

- State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy-List.aspx
- USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

5. POLICY

SUIT is committed to establishing policy that incorporates industry standards and best practices while using technically sound methodology to mount an efficient and effective incident response. This policy establishes the minimum requirements for SUIT to respond to a cybersecurity incident.

5.1 Establish and Maintain Cybersecurity Incident Response Capability

SUIT must have a security incident management plan as directed within this policy to include any technical capability required to address any compromise and remediation of a cybersecurity incident.

NOTE: This policy does not address security incidents that do not have a cybersecurity component, such as the theft of non-computer office supplies or a physical altercation between employees

5.2 Incident Tracking and Documentation

Information security incidents shall be documented and tracked in accordance with the requirements shown in the table below

#	Name	Requirement
A	Incident Tracking	All incidents will be recorded and reported.
B	Retention Period	Records of incidents will be maintained for at least a period of 3 years, or longer as required under relevant regulations.
C	Tracking Method	Where possible an automated system or platform will be used to track incidents. This system will allow for: • Tracking of the status and disposition of individual incidents • Reporting to SUIT • Correlating between incidents • Tracking and reporting of IR Key Performance Indicators (KPIs)

5.3 Staffing and External Support

SUIT will establish and appoint members for information security response staff necessary for a reasonable response to a cybersecurity incident in accordance with the requirements of this policy. The staff responsible for responding to cybersecurity incidents will be maintained in the associated incident response procedures. In addition, current information on key SUIT vendors will be documented and referenced in the incident response procedures so that solution-specific consulting and support vendors can be rapidly obtained during an incident.

5.4 Security Incident Management Plan

SUIT will establish and maintain a Security Incident Management Plan to comply with the provisions listed in the table below.

#	Name	Requirement
A	Process	Incorporate technically sound methodology to be used by the agency during information security incidents, which shall be flexible enough to account for a wide-range of potential cybersecurity incident types.
B	Organizational Structure, Roles & Responsibilities	Define and describe an organizational structure, including: ▪ Identifying the agency Incident Response Coordinator ▪ Defining oversight and management team(s)/roles ▪ Defining roles and responsibilities for team members o Including the identification of those individuals authorized to communicate to the public, if required. ▪ Defining approval authorities for all major incident response decisions
C	Required Technology Support	Define and describe the hardware and software necessary to conduct incident response, as well as the required deployment of such assets to support response efforts.
D	Incident Severity Levels	Incorporate incident severity levels as described in Section 4.5.
E	KPIs	Define and describe the key performance indicators that will be used to measure incident response performance.
F	Review and Revision	Review and revise this plan annually and as needed if deficiencies are noted after a major incident, a training exercise, or an audit finding.
G	Coordination with State Agencies	Establish coordination with USM and state agencies in accordance with mission/business roles and severity.
H	Coordination with Other Plans	Identify guidelines for coordinating with related plans, including but not limited to disaster recovery and business continuity plans.
I	Legal Counsel	Identify guidelines for any conditions requiring the advice of legal counsel to ensure that legal and regulatory obligations are assessed and met during incidents.
J	Approval	Requires written approval from the CIO, or a delegated authority.
K	Reporting	Determine guidelines for interim and post-incident report contents.
L	Internal Notification	Data owners will establish and maintain response strategies that incorporate SUIT notification requirements as shown in Section 4.7.
M	Breach Notifications	Data owners will establish and maintain response strategies for handling breach notification requirements as shown in Section 4.8.

5.5 Cybersecurity Incident Severity Levels

Cybersecurity levels will be defined by SUIT and depending on the severity level may be elevated to USM or state agencies.

5.6 Exercises and Training

SUIT will conduct incident response exercises and trainings in accordance with the requirements show in the table below.

#	Name	Requirement
A	Organization-wide Exercises	Conduct an organization-wide, table-top incident response exercises at least annually.
C	Post-exercise Reports	Reports will be drafted for all exercises that will include any capability gaps identified along with other lessons learned.
D	Training Events	Exercises will include sufficient training in order to enable participants to understand and execute their functions/roles.

5.7 Incident Reporting and Notification

Information security incidents will be reported in accordance with SUIT notification process guidelines outlined in incident response procedures.

5.8 Breach Notifications

2013 Maryland Code §10-1301 (Md. State Govt. Code §§ 10-1301 to -1308) defines the breach requirements of Personally Identifiable Information. Under the Maryland statute, a breach is considered to be any "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a unit." Additionally, if a unit discovers or is notified of a breach, it must conduct in good faith a reasonable and prompt investigation to determine whether the unauthorized acquisition of personal information of the individual has resulted in or is likely to result in the misuse of the information.

After an investigation is concluded, the unit must determine if notification is required under the specific circumstances. A unit or nonaffiliated third party is not required to notify an individual of a breach if the personal information of the individual was secured by encryption or redacted and the encryption key has not been compromised or disclosed. See 2013 Maryland Code §§101301-1308 for further information on notification requirements.

Incidents involving the compromise of personal information (as defined under State Government Article 10-1031 above) must be reported to the USM office of the CIO.

NOTE: This policy provides guidance for compliance with specific portions of the Maryland Code §§10-1301-1308, but does not supplement, replace or supersede the Maryland law itself. Executive agencies and the associated vendors or contractors are responsible for independently complying with all provisions of Maryland law and other regulations/standards that affect specific types of Confidential Data, such as those required under HIPAA. PCI DSS, or IRS-1075

6. EXEMPTIONS

If an exemption from this policy is required, an SUIT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted.

7. DEFINITIONS

Term	Definition
Cybersecurity Incident	A verified event or set of events that has or may result in a change to the confidentiality, availability or integrity of University information systems, networks, or data, and for which a directed response may be required to mitigate the associated damage or risk. An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies may also be considered an incident.
Data Owner	Official(s) with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

8. ENFORCEMENT

SUIT is responsible for managing cybersecurity incident response policy for the University. Any systems under the policy authority of SUIT with requirements that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.