MISSISSIPPI

Mississippi Department of
Information Technology Services

2020

ENTERPRISE SECURITY PROGRAM

TABLE OF CONTENTS

ENTERPRISE SECURITY PROGRAM 1
Program Authority 1
Program Structure 1
Reference Information 2
Applicability 2
PROGRAM ROLES AND RESPONSIBILITIES 3
ITS Executive Director 3
ITS Security Services Division 3
Information Security Council 4
State Agency 4
PROGRAM FRAMEWORK 5
PROGRAM COMPLIANCE 6
ENTERPRISE SECURITY GOVERNANCE 8
Policy and Standards Review Process 8
Policy and Standards Exception Process 9
ITS CONTACT INFORMATION 10

ENTERPRISE SECURITY PROGRAM

Program Authority

In the 2017 Legislative Session, the Mississippi Legislature passed House Bill 999 that created a new section of Mississippi Code (25-53-201) for the advancement of the state government enterprise approach to cybersecurity.

To fulfill the statutory requirements in Mississippi Code Ann. 25-53-201 for cybersecurity, the State of Mississippi will have a comprehensive cybersecurity program (the Enterprise Security Program) to provide coordinated oversight of the cybersecurity efforts across all state agencies, including cybersecurity systems, services and development of policies, standards and guidelines.

The Mississippi Department of Information Technology Services (ITS) will administer the Enterprise Security Program to execute the duties and responsibilities of Mississippi Code Ann. 25-53-201.

Program Structure

It is important for stakeholders across all areas of state government to have a clear understanding of the authority for the Enterprise Security Program, its scope, and key roles and responsibilities. Under Mississippi Code Ann. 25-53-201, the Executive Director of ITS has both the responsibility and authority to establish and maintain the Enterprise Security Program. The Program will coordinate and oversee enterprise cybersecurity efforts that include defining enterprise cybersecurity systems and services and acquiring and operating enterprise technology solutions to improve the cybersecurity posture in the function of any agency, institution or function of state government as a whole.

To implement the activities and responsibilities of the Enterprise Security Program, the Executive Director of ITS has assigned the oversight of the Enterprise Security Program to the ITS Security Services Division. Through the Information Security Council, state agencies will help plan, develop and implement enterprise security objectives.

Reference Information

- **House Bill 999, 2017 Regular Legislative Session:** Enterprise Security Program; establish to provide policies for cybersecurity safety across state government
- **Mississippi Code Ann. 25-53-201**

Applicability

Enterprise Security Program requirements are applicable to all state agencies of state government and must be carried out by all employees within the state agencies. State agency heads, Chief Information Officers, agency security leaders, and their designees must be aware of program requirements. Program requirements must also be included in any arrangement with third parties that handle, store, or transfer State of Mississippi Data.

PROGRAM ROLES AND RESPONSIBILITIES

ITS Executive Director

- Ensures that ITS maintains the Enterprise Security Program
- Ensures that enterprise technology solutions and enterprise security policies and standards for all state data and IT resources support the States' IT security goals, direction, and objectives
- Delegates the oversight of the Enterprise Security Program to the ITS Security Services Division
- Monitors the overall effectiveness of the Enterprise Security Program
- Ensures that ITS complies with all aspects of the Enterprise Security Program directed at state agencies

ITS Security Services Division

- Administers the Enterprise Security Program to execute the statutory duties and responsibilities
- Maintains the Enterprise Security Policy
- Implements enterprise technology solutions and security standards and policies capable of improving the cybersecurity posture in the function of any agency, institution or function of state government as a whole
- Provides ongoing analysis of enterprise cybersecurity systems and services costs, facilities, and systems within state government
- Develops enterprise plans for the use of enterprise cybersecurity systems and services
- Develops cybersecurity-related policies, procedures, and guidelines
- Organizes an advisory council of Information Security Officers from each state agency and coordinates the activities of the advisory council to provide education and awareness, identify cybersecurity-related issues, set future direction for cybersecurity plans and policy, and provide a forum for inter-agency communications regarding cybersecurity
- Requires cooperative utilization of cybersecurity systems and services by aggregating users

- Facilitates sharing of cybersecurity information among all agencies

Information Security Council

- Assists with the planning, development, and implementation of cybersecurity initiatives
- Identifies cybersecurity-related issues
- Assists in setting future direction for cybersecurity plans and policy
- Reviews and provides recommendations for exceptions to enterprise security policies and standards
- Participates in cybersecurity information sharing among agencies

State Agency

- Ensures the security of all data and IT resources under the agency's purview, irrespective of the location of the data or resources
- Ensures that an agency-wide cybersecurity program plan is in place and administered by a designated information security officer
- Complies with the requirements established by the Enterprise Security Program, to the extent that they apply
- Ensures agency staff participate in the Information Security Council
- Participates in all Enterprise Security Program initiatives and services in lieu of deploying duplicate services specific to the agency
- Implements policies and standards to ensure that all of the agency's data and IT resources are maintained in compliance with state and federal laws and regulations, to the extent that they apply
- Implements appropriate cost-effective safeguards to reduce, eliminate or recover from identified threats to data and IT resources
- Ensures that internal assessments of the agency security program are conducted

PROGRAM FRAMEWORK

The Enterprise Security Program utilizes the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the security controls defined in the 800 series of publications by NIST, and the CIS Critical Security Controls. This Program consists of five fundamental areas that contain enterprise-level policies listed below. Each functional area may be supported by one or more Enterprise Security Standards. These standards will be documented separately; however, they will all be governed by the Program.

PROGRAM COMPLIANCE

State agencies must monitor and document compliance to the enterprise security policies and standards published by the Enterprise Security Program as well as all applicable federal, state, and regulatory requirements.

The Program will assess and monitor the cybersecurity effort and provide updates to the ITS Executive Director and other appropriate state government stakeholders. ITS activities include the following:

- Identify and measure Key Performance Indicators (KPI)
- Communicate status and progress to the appropriate state government stakeholders
- Evaluate the Enterprise Security Program for effectiveness
- Evaluate and report state agency participation to the appropriate state government stakeholders
- Collaborate with the Office of the State Auditor in audit compliance

The Office of the State Auditor (OSA), as part of their normal agency information systems auditing activities, will review how well agencies comply with security policies. OSA activities include the following:

- Consider the Enterprise Security Program policies and standards in the review of the systems, processes, and procedures that they examine
- Determine if special audits of an agency's information system processing are warranted, and if so, proceed under their existing authority
- Request and review copies of an agency's IT Security Risk Assessment documentation
- Identify any areas of non-compliance and instruct the agency and/or ITS to take necessary steps to become compliant

State agencies will assess, monitor, and report on their own compliance to the Program and other regulatory requirements. State agencies will do this through the following activities:

- Align resources for and in cooperation with OSA compliance assessments and the Program

- Maintain a detailed copy of the results of their internal and third party reviews, assessments, or audits and plans for correcting significant deficiencies identified
- Provide, as requested, the OSA a detailed copy of all results from any internal, third party, or Federal regulatory assessment, evaluation, and audit of information systems
- Adhere to the reporting requirements of the Program
- Follow the exception process for any area they are not in compliance with the Program

Enterprise Security Governance

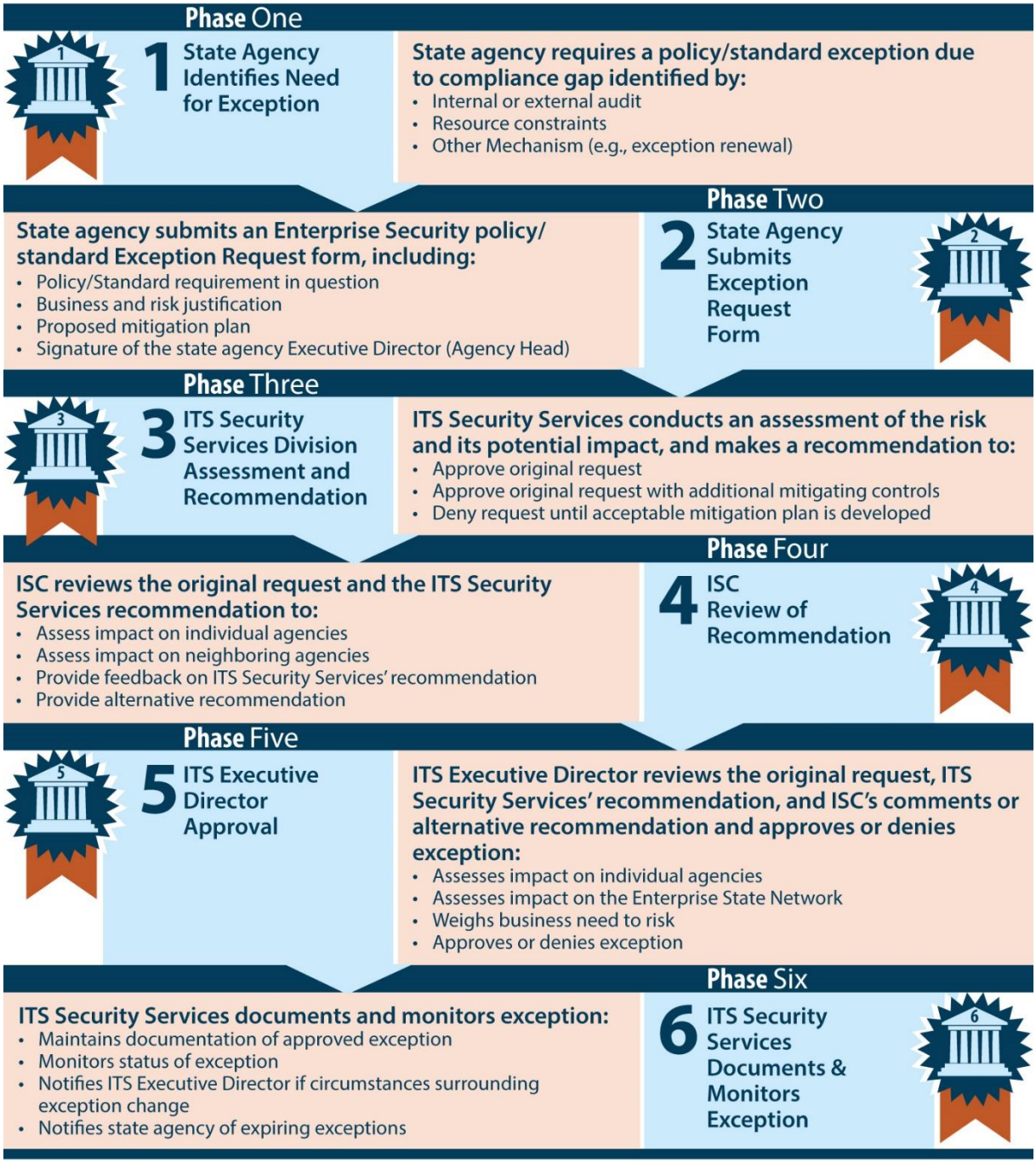
Periodic review of the enterprise policies and standards for applicability and appropriateness will be conducted on an as needed basis. ITS will collaborate with the Information Security Council when enterprise policies and standards are reviewed.

Policy and Standards Review Process

The following process will be used to create, change, periodically review, and approve enterprise security policies and standards.

Policy and Standards Exception Process

The following process will be used to consider exceptions to Enterprise Security Program requirements, policies, and standards.



ITS Contact Information

Executive Director	Dr. Craig P. Orgeron (601) 432-8000 craig.orgeron@its.ms.gov
Chief Administrative Officer	Michele Blocker (601) 432-8111 michele.blocker@its.ms.gov
Chief Operations Officer	Roger Graves (601) 432-8092 roger.graves@its.ms.gov
Data Services	Laura Pentecost (601) 432-8191 laura.pentecost@its.ms.gov
Information Systems Services	David Johnson (601) 432-8126 david.johnson@its.ms.gov
Internal Services	Holly Savorgnan (601) 432-8102 holly.savorgnan@its.ms.gov
Security Services	Jay White (601) 432-8180 jay.white@its.ms.gov
Strategic Services	Debra Brown (601) 432-8128 debra.brown@its.ms.gov
Telecommunications Services	Steven Walker (601) 432-8004 steven.walker@its.ms.gov
Mississippi Department of Information Technology Services	3771 Eastwood Drive Jackson, MS 39211 (601) 432-8000

Dr. Craig P. Orgeron, Executive Director

3771 Eastwood Drive
Jackson, Mississippi 39211
Telephone (601) 432-8000
Fax (601) 713-6380
Web site: www.its.ms.gov
State Portal: www.mississippi.gov