ITS Access Control Policy
Notice of Approval

Mississippi Department of Information Technology Services	**Doc Ref Number:** ITS-PSG-3006	
	Title: ITS Access Control Policy	
	Document Type: ITS Agency	
	Domain: Security | Compliance	**Status:** Pending Approval
	Effective Date: 10-11-2017	**Revision Date:** 10-11-2017

Notice is hereby given, that the above specified document meets the requirements of the Mississippi Department of Information Technology Services Policies, Standards and Guidelines Program, defined in ESW-PSG-1001, thereby warranting approval for implementation, effective immediately.

Executive Director
Mississippi Department of
Information Technology Services

October 11, 2017
Date of Signature

Mississippi Department of Information Technology Services	**Doc Ref Number:** ITS-PSG-3006	
	Title: ITS Access Control Policy	
	Document Type: ITS Agency	**Page:** 1 of 4
	Domain: Security | Compliance	**Status:** Approved
	Effective Date: 10-11-2017	**Revision Date:** 10-11-2017

1. AUTHORITY

The Mississippi Department of Information Technology Services (ITS) shall issue recommended strategies and goals for the effective and efficient use of information technology and services in state government (§ 25-53-29(2)). Additionally, ITS, shall publish written planning guides, policies and procedures for use by agencies and institutions in planning future electronic information service systems (§ 25-53-29(1) (b)).

2. PURPOSE

The purpose of this Information Technology Services (ITS) Access Control Policy is to compliment all other physical and logical security policies and procedures for the protection of critical hardware, software, and data within the State of Mississippi ITS Data Centers. Access Control is considered the first barrier in protecting critical IT resources and data.

3. SCOPE

The ITS Access Control Policy is limited to electronic card access and physical key access to ITS buildings A, B, and C located on the Eastwood campus, REL Co-processing Data Center, and access controlled equipment rooms and cabinets under ITS purview. The Policy includes; keys required to access rooms, server cabinets, mainframe cabinets, network closets, electrical closets, and all other secured areas where computing, storages, network, and related devices are maintained by ITS.

4. POLICY

The State of Mississippi, Information Technology Services, shall have effective procedures for physical building security to compliment all other physical and logical procedures for protection of hardware, software, networking, and support equipment that stores and processes data for authorized agencies of the State of Mississippi.

5. STANDARDS

5.1 Information Technology Services shall ensure an effective method for the issuing and collecting of all physical keys and electronic access cards.

5.2 A record of all issued, returned, and lost or stolen keys and electronic access cards including name of last assigned shall be maintained for at least 5 years.

5.3 A record of all electronic card swipes shall be maintained for at least 5 years.

5.4 Access shall be issued only to authorized employees, contractors and customers of ITS.

5.5 The assigned key and electronic access card inventory logs, shall at a minimum, include the access holders name and shall be updated each time access is assigned and a copy given to ITS Human Resources with each change and at least monthly.

5.6 Unassigned keys and access cards shall be maintained in secured locked cabinets and inventoried at least monthly.

5.7 Human Resources shall collect all assigned keys and access cards when an employee's access is no longer needed, employee leaves, or terminated.

5.8 All keys and electronic access cards remain the property of State of Mississippi ITS and shall not be copied or duplicated.

5.9 ITS staff with assigned DFA, Department of Finance, access cards shall follow the Policy and Standards provided by DFA. ITS Human Resources shall authorize and facilitate the process for request and termination of DFA access cards required for ITS staff.

5.10 ITS staff with authorized access to the Cspire, ITS Ancillary Data Center, shall follow the Policy and Standards provide by Cspire. ITS Human Resources and the ITS Data Center Infrastructure Manager shall authorize and facilitate the process for request and termination of Cspire, ITS Ancillary Data Center, access required for ITS staff.

6. GUIDELINES

6.1 The assigned, key and access card inventory logs should include additional information such as shown in the example log; "ITS Data Center Access Control Log".

6.2 A designated access control administrator should be designated for executing and enforcing this policy for building A (main employee office building) on the Eastwood campus. The administrator should control all door keys for building A, all electronic access cards, and access updates for the ITS campus.

6.3 A designated access control administrator should be designated for executing and enforcing this policy for buildings B and C (main data center and electrical facility) on the Eastwood campus, REL Co-processing Data Center, and access to controlled equipment rooms and cabinets under ITS purview. The administrator should control all door keys and badge access

to the facilities listed above.

6.4 The ITS Chief Operations Officer and/or Chief Administrative Officer should authorize permanent vendor/contractor access to facilities under ITS purview.

7. REFERENCES

§ 25-53-29 (2)
§ 25-53-29 (1) (b)

8. ATTACHMENTS

ITS Data Center Access Control Log

ITS Data Center Access Control Log

Key No. (unique or master)	Key Purpose (provides access to)	Key Holder Name	Key Holder Signature	Supervisor / Manager	Date Issued	Date Returned