COMPLIANCE COMPONENT

DEFINITION	
Name	Securing Remote Connections
Description	Securing Remote Connections is necessary to ensure the confidentiality, integrity and availability of information transmitted via the Internet.
Rationale	Remote access poses a higher risk to State of Missouri information systems. Due to the growth of remote work, there is an increasing number of people who need secure remote access.
Benefits	• Provides a means of securing a system that is connected to an agency via a public provider

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Technical Controls
Specify the Technology Area Name	Remote Access Controls
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	

State the Guideline, Standard or Legislation	<u>Securing Remote Connections</u>
	• Only agency-approved equipment may be remotely connected to State of Missouri systems.
	• Endpoint protection software must be installed and up to date on devises utilized for remote connections.
	• A firewall must be installed and properly configured on all remotely connected systems (see the Firewall Rules Compliance Component)
	• Computers connected to the State of Missouri systems shall not simultaneously connect to any other network via another network device.
	  ○ Split-tunneling must not be enabled on the VPN.
	  ○ Shares between the agency systems and non-agency systems must be disabled when the remote device is connected to any State of Missouri system.
	• Data should not be stored on remote devices.
	• <u>Agency approval is</u> required before any user may connect remotely to the agency network.
	• Remote connections must meet the cryptography compliance component requirements (see the Cryptography CC)
	• Remote connections require multi-factor authentication.

Document Source Reference #	NIST Special Publication 800-46, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, Rev. 2 (July 2016)		
Compliance Sources			
Name	NIST, CERT®Coordination Center	*Website*	csrc.nist.gov, www.cert.org
Contact Information			
Name		*Website*	
Contact Information			
KEYWORDS			
List Keywords	Broadband, Cable, Digital Subscriber Line (DSL), Wireless, Broadband over Power Line (BPL), Power Line Communications (PLC), Satellite, Internet, Virtual Private Network (VPN),		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Sunset Date			

COMPONENT SUB-CLASSIFICATION		
Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☐ *Variance*		
☐ *Conditional Use*		

Rationale for Component Classification	
Document the Rationale for Component Classification	
Migration Strategy	
Document the Migration Strategy	
Impact Position Statement	
Document the Position Statement on Impact	
CURRENT STATUS	
Provide the Current Status	☐ *In Development* ☒ *Under Review* ☐ *Approved* ☐ *Rejected*

AUDIT TRAIL			
Creation Date	03/31/2005	*Date Approved / Rejected*	11/08/05
Reason for Rejection			
Last Date Reviewed	06/06/2024	*Last Date Updated*	06/21/2024
Reason for Update	Vitality		