



COMPLIANCE COMPONENT

DEFINITION	
<i>Name</i>	Inactivity Controls
<i>Description</i>	Inactivity controls protect against unauthorized system usage by disabling an electronic device or session after a pre-determined time of inactivity.
<i>Rationale</i>	Appropriate inactivity safeguards must be used to protect against unauthorized access to or use of information, data, and software resident on computers, peripheral devices, and storage media. Inactivity controls are particularly necessary in open offices where there are no walls and many people leave their computers on and available for anyone who happens to walk by. Inactivity controls can also be used to protect information or data transmitted over communication lines or networks.
<i>Benefits</i>	<ul style="list-style-type: none"> • Protect against unauthorized disclosure • Protect against unauthorized system usage
ASSOCIATED ARCHITECTURE LEVELS	
<i>Specify the Domain Name</i>	Security
<i>Specify the Discipline Name</i>	Technical Controls
<i>Specify the Technology Area Name</i>	Logical Access Controls
<i>Specify the Product Component Name</i>	
COMPLIANCE COMPONENT TYPE	
<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	
COMPLIANCE DETAIL	
<i>State the Guideline, Standard or Legislation</i>	<ul style="list-style-type: none"> • To maintain the confidentiality and integrity of information and information systems, users shall lock the system, log-out or invoke a password-protected screen saver before leaving any computer or electronic device unattended. • If there has been no activity on a computer or electronic device for a maximum of fifteen (15) minutes, the computer or electronic device shall be locked. Re-establishment of the computer or electronic device shall take place only after the user has renewed access via the proper authentication, such as a password. • While computing, user sessions are locked after fifteen (15) minutes of inactivity. Users will be required to re-authenticate to continue their sessions after screen lockout due to inactivity.
<i>Document Source Reference #</i>	NIST SP 800-53, Rev. 5 IRS Publication 1075, revision 11-2021

Compliance Sources			
<i>Name</i>	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	<i>Website</i>	http://csrc.nist.gov/
<i>Contact Information</i>	inquiries@nist.gov		
<i>Name</i>	Internal Revenue Service	<i>Website</i>	http://www.irs.gov/
<i>Contact Information</i>	SafeguardReports@irs.gov		
KEYWORDS			
<i>List Keywords</i>	Idle, time out, login, log-out, screen saver, session, lockout, inactivity, re-authenticate.		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i>	<input checked="" type="checkbox"/> <i>Current</i>	<input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>
<i>Sunset Date</i>			
COMPONENT SUB-CLASSIFICATION			
<i>Sub-Classification</i>	<i>Date</i>	<i>Additional Sub-Classification Information</i>	
<input type="checkbox"/> <i>Technology Watch</i>			
<input type="checkbox"/> <i>Variance</i>			
<input type="checkbox"/> <i>Conditional Use</i>			
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>			
Migration Strategy			
<i>Document the Migration Strategy</i>			
Impact Position Statement			
<i>Document the Position Statement on Impact</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i>	<input type="checkbox"/> <i>Under Review</i>	<input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>
AUDIT TRAIL			
<i>Creation Date</i>	03/06/2003	<i>Date Approved / Rejected</i>	03/24/2003
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>	09/21/2022	<i>Last Date Updated</i>	09/30/2022
<i>Reason for Update</i>	Vitality		