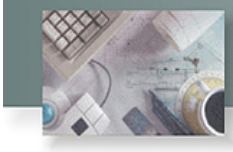

Compliance Component

DEFINITION	
Name	Date/Time Controls
Description	Restrictions based on time and day bolsters the control environment. The intent is to require more than simple access controls, normally based on user-IDs and passwords.
Rationale	Hackers are most active at night, just when systems are sparsely staffed, if staffed at all. If users stay logged on, hackers can attack their network assets and use them to attack other systems.
Benefits	• Reduces the amount of time the account is open to unauthorized access.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Logical Access Controls
List Product Component Name	

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

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	• Whenever possible access control should constrain the user to use of the system within a limited working day and only on normal working days of the week (some systems even make allowances for denying access on public holidays). Such a restriction helps prevent misuse of the system out of hours by an employee (a cleaner, perhaps) or by a hacker (who often rely on out-of-hours access to avoid detection by legitimate users). • Similarly, restrictions should be placed on the workstations the user can employ and on the applications that can be run on a particular workstation. This measure is particularly useful in limiting very privileged activities (system support, security administration, for example) to certain workstations and thus putting a physical barrier in the way of a would-be attacker.
Document Source Reference #	NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs) CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/)

Standard Organization			
Name	Carnegie Mellon University, CERT/Coordination Center (CERT/CC)	*Website*	www.cert.org
Contact Information	cert@cert.org		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	Access, times, work schedule, hours, system availability, after hours		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
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	3/6/2003	*Date Accepted / Rejected*	03/24/2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			