

## Application Security Baseline Requirements and Controls – Technical

Id Num	Baseline Technical Requirements	Tier (1)	Tier (2)	Tier (3)
<b>(1) Access Controls</b>				
1.1	The application system shall support the management of system accounts	X	X	
1.2	The application system shall provide the capability of terminating temporary and emergency accounts based on timeframes specified by the system owner	X	X	
1.3	The application system shall provide the capability to disable inactive accounts	X	X	
1.3.1	The application system shall provide the capability to determine if accounts have been inactive 30 days or more	X	X	
1.4	The application system shall provide the capability to audit account creation	X	X	
1.4.1	The application system shall provide the capability to audit account modifications.	X	X	
1.4.2	The application system shall provide the capability to audit account disabling.	X	X	
1.4.3	The application system shall provide the capability to audit account termination.	X	X	
1.4.4	The application system shall provide the capability to notify appropriate individuals of account auditing activities	X	X	
1.5	The application system shall provide access enforcement capability	X	X	
1.5.1	The application system shall restrict access to privileged functions deployed in hardware	X	X	
1.5.2	The application system shall restrict access to privileged functions deployed in software	X	X	
1.5.3	The application system shall restrict access to privileged functions deployed in firmware	X	X	
1.5.4	The application system shall restrict access to privileged functions to explicitly authorized personnel.	X	X	
1.6	The application system shall provide the ability to control the flow of information	X		

<b>1.6.1</b>	The application system shall enforce assigned authorizations for controlling the flow of information within the system	<b>X</b>		
<b>1.6.2</b>	The application system shall enforce assigned authorization for controlling the flow of information between interconnected systems	<b>X</b>		
<b>1.7</b>	The application system shall provide the capability to enforce separation of duties	<b>X</b>	<b>X</b>	
<b>1.8</b>	The application system shall be capable of restricting users to the most restrictive access needed to perform job.	<b>X</b>	<b>X</b>	
<b>1.9</b>	The application system shall provide the capability to monitor unsuccessful login attempts	<b>X</b>	<b>X</b>	
<b>1.9.1</b>	The application system shall provide the capability to enforce a limit on the number of login attempts by user, system, or process.	<b>X</b>	<b>X</b>	
<b>1.9.2</b>	The application system shall provide the capability to enforce a limit on the number of login attempts within timeframes designated by the application owner.	<b>X</b>	<b>X</b>	
<b>1.9.3</b>	The application system shall provide the capability of locking the accounts of users, systems, or process that exceeds the authorized number of login attempts.	<b>X</b>	<b>X</b>	
<b>1.9.4</b>	The application system shall provide the capability of locking the accounts of users, systems, or processes that attempt to access the application after authorized timeframes.	<b>X</b>	<b>X</b>	
<b>1.9.5</b>	The application system shall provide administrators the capability to unlock the accounts.	<b>X</b>	<b>X</b>	
<b>1.10</b>	The application system shall provide the capability of customized login banner information.	<b>X</b>	<b>X</b>	
<b>1.11</b>	The application system shall provide the capability to limit concurrent login sessions	<b>X</b>		
<b>1.12</b>	The application system shall provide the capability to lock the system after a period of inactivity as determined by policy	<b>X</b>	<b>X</b>	
<b>1.13</b>	The application system shall provide the capability to open a locked session with	<b>X</b>	<b>X</b>	

	appropriate authenticated credentials.			
<b>1.13.1</b>	The application system shall provide the capability for users to the lock sessions upon demand.	<b>X</b>	<b>X</b>	
<b>1.14</b>	The application system shall provide session termination capability			
<b>1.14.1</b>	The application system shall provide the capability of terminating remote sessions due to inactivity	<b>X</b>		
<b>1.14.2</b>	The application system shall provide the capability of terminating local sessions due to inactivity	<b>X</b>		
<b>1.15</b>	The application system shall provide the capability to review user activities on the system.	<b>X</b>	<b>X</b>	
<b>1.16</b>	The application system shall provide the capability to determine the actions that can be performed without identification and authentication	<b>X</b>	<b>X</b>	
<b>1.17</b>	The application system shall provide the capability to encrypt remote sessions	<b>X</b>	<b>X</b>	
<b>(2) Auditing and Accountability</b>				
<b>2.1</b>	The application system shall provide the capability to produce an audit trail	<b>X</b>	<b>X</b>	
<b>2.1.1</b>	The application system shall provide the capability to manage the selection of events to be audited	<b>X</b>	<b>X</b>	
<b>2.2</b>	The application system shall provide the capability to manage the content of the auditing records	<b>X</b>	<b>X</b>	
<b>2.3</b>	The application system shall provide a warning when audit record storage reaches maximum capacity.	<b>X</b>	<b>X</b>	
<b>2.3.1</b>	The application shall produce a real time alert if audit event failure occurs	<b>X</b>		

2.4	The application system shall provide the capability to generate reports based on desired selected events	X	X	
2.5	The application system shall apply time stamps to auditable events	X	X	
2.6	The application system shall provide the capability to protect audit logs from unauthorized access	X	X	
2.6.1	The application system shall provide the capability to protect audit logs from unauthorized modification	X	X	
2.6.2	The application system shall provide the capability to protect audit logs from unauthorized deletion	X	X	
2.7	The application system shall provide the capability of tracing auditable events to the individual taken the action	X	X	
<b>(3) Identification and Authentication</b>				
3.1	The application system shall provide the capability of uniquely identifying and authenticating users (people, processes, and devices)	X	X	
3.1.1	The application system must uniquely identify and authenticate users (people, processes, and devices) before a connection can be established.	X	X	
3.2	The application system shall provide the capability to obscure authentication information as it is being verified.	X	X	
3.3	The application system shall provide the capability to encrypt the authentication information as it is being verified.	X	X	

<b>(4) System and Communication Protection</b>				
<b>4.1</b>	The application system must isolate security functions from non-security functions	<b>X</b>	<b>X</b>	
<b>4.2</b>	The application system must unauthorized and unintended transfer of information via shared resources.	<b>X</b>	<b>X</b>	
<b>4.3</b>	The application system must encrypt data transmissions using a FIPS 140-2 algorithm	<b>X</b>		