

The application user interface must be either physically or logically separated from data storage and management interfaces.  
The application must set the HTTPOnly flag on session cookies.  
The application must not expose session IDs.  
The application must destroy the session ID value and/or cookie on logoff or browser close.