|  |  |  |
| --- | --- | --- |
| Requirement | Pass | Fail |
| Does the application uniquely identify each user with a unique ID? |  |  |
| Do all interfaces of the application that are accessed for performing any actions can recognize the user ID? |  |  |
| Does application associate the process with the user ID ? |  |  |
| Does application have the capability to automatically disable an identiﬁer if it remains inactive for a speciﬁed time period (e.g., 90 days)? |  |  |
| Does application maintain a list of security attributes for each user e.g user ID, group memberships, access control privileges, authentication information? |  |  |
| Does application store information used for the authentication purposes in a secure manner e.g by using public and widely accepted crypto algorithms? |  |  |
| Does application provide a feedback to the user during the authentication procedure other than “invalid”? |  |  |
| Does application have the ability to authenticate itself to the user and to the other systems during a session establishment? |  |  |
| Does application have the ability to reauthenticate a user during an active session ? |  |  |
| Does application divulge in a clear text the static authenticator for one of the users to any other user ? |  |  |
| On ﬁrst use - Does application prompt a user to change the initial password and deny access if the user does not comply ? |  |  |
| Does application allow users to change their own password later on at any time ? |  |  |
| Does application offer a credential aging feature that forces users to periodically change static authentication information ? |  |  |
| Does application require re-authentication by the user at the time of an attempted password change? |  |  |
| Does application provide a mechanism to prevent a password re-use? |  |  |
| Does application force that the authentication information are of: minimum length, alphabetic characters and numeric or special characters ? |  |  |
| Does application allow access to the system resources without checking the assigned rights and privileges of the user? |  |  |
| Does several consecutive incorrect login attempts generate an alarm and account lock out? |  |  |
| Upon successful session establishment – Does application log the date and time of the last successful login ? |  |  |
| Does application automatically terminate a user session after some period of time? |  |  |
| Does application have features to assign user and group privileges? |  |  |
| Does application provide a resource control mechanism that grants or denies access to the resources based on a user and interface privileges? |  |  |
| Does application provide a capability for the administrator to specify limits on the number of concurrent logon sessions for a given user? |  |  |
| Does application maintain an audit log that provides an adequate information for establishing audit trails in the case of a security breach? |  |  |
| Does application maintain the conﬁdentiality of authenticators? |  |  |
| Does application provide an administrator with the ability to retrieve, print and copy a content of the audit logs? |  |  |
| Does application protect the audit logs from unauthorized access, modiﬁcation or deletion. |  |  |
| Does application protect a system and a user information from unauthorized disclosure while stored or in transit? |  |  |
| Does application provide a secure key storage ? |  |  |
| Does application implement a standard key generation algorithm that generates non-predictable values? |  |  |
| Does application provide a secure integrity checking capabilities through the interface between a user and a system? |  |  |
| Does application provide mechanisms to detect communication security violations? |  |  |
| Does application deny an access unless a user has permission to access the resource |  |  |
| Does application provide a mechanism to define privileges? |  |  |
| Does application have a capability to prevent an access to the potentially damaging commands (e.g., delete all ﬁles) from users who do not need to execute such commands on a regular basis? |  |  |
| Does application have a capability to impose an access control on the basis of functions such as Create, Read, Update, and Delete (CRUD)? |  |  |
| Does application provide a notice to the individuals about the entity’s privacy policies and procedures? |  |  |
| Are individuals informed about the choices available to them with respect to the collection, use, and disclosure of personal information? |  |  |
| Is implicit or explicit consent obtained from the individuals at or before the time personal information is collected or soon after? |  |  |
| Does application use a personal information only for the purposes identiﬁed in the notice? |  |  |
| Does application retain a personal information longer than necessary? |  |  |
| Does application’ s privacy notice disclose what type of personal information is collected as well as sources and methods? |  |  |
| Does application anonymize, dispose of or destroy the personal information that are no longer needed in a manner that prevents loss, theft, misuse, or unauthorized access ? |  |  |
| Does application disclose personal information to the third parties only for the purposes described in the notice, and for which the individual has provided implicit or explicit consent? |  |  |