|  |  |  |
| --- | --- | --- |
| **Test Case No.** | **Test Case Name** | **Asset** |
| REQ-STC-001 | The Application shall support the use of anti-malware mechanism | Tablet |
| REQ-STC-002 | The Application shall provide secure tunnel Communications channel | Tablet  SM Device  NSA |
| REQ-STC-003 | Only Stryker made/ authenticated devices should be able to communicate with SM device and tablet. | Tablet  SM Device |
| REQ-STC-004 | The application shall be allowed to upgrade the tablet application. | Admin |
| REQ-STC-005 | Application shall have the User Management Screen to configure and manage the users as per the roles. | Admin |
| REQ-STC-006 | The Application shall be validated by using invisible captcha during login. | NSA |
| REQ-STC-007 | Invalid login creds, only 3 attempts left. | Admin  NSA |
| REQ-STC-008 | System shall store patient id in anonymized fashion. | Admin |
| REQ-STC-009 | Error msg: Something went wrong with API operation try again / contact API admin. | Admin  NSA |
| REQ-STC-010 | For sensitive data at rest, identification & proper encryption mechanism needs to be designed & implemented | Tablet  Cloud db |
| REQ-STC-011 | Secure sensitive data in the channel flow using strong encryption | Tablet  Admin |
| REQ-STC-012 | Weak algorithms such as DES, RC4, etc.. should be avoided and usage of strong algorithms such as AES, RSA, etc.. are recommended | Tablet  Cloud db |
| REQ-STC-013 | Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended. | Tablet  Cloud db |
| REQ-STC-014 | If database access using keys/certificates, their generation & storage should be done securely. | Tablet  Cloud db |
| REQ-STC-015 | Weight and patient data in the database shall be available upto 6 months. | NSA |
| REQ-STC-016 | User shall find the overall system flow in the User Manual document. | NSA |
| REQ-STC-017 | The application will be used by the Stryker Installation and service teams. | Admin |