

**Basic Hardening and Hygiene Checklist for Telecom Network Element**

**MBSS Type: Telecom MBSS Generic.**

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Item** | **Details** |
| 1 | OEM |  |
| 2 | Node Type |  |
| 3 | Native or Virtual | Virtual |
| 4 | Hardware Platform |  |
| 5 | Software Version |  |
| 6 | Circle Name |  |
| 7 | Location Name | Manesar |
| 8 | IP Address |  |
| 9 | Host Name |  |
| 10 | OEM Spoc  (Name, E-mail & Mobile No.) |  |
| 11 | MS Operation Spoc (Name, E-mail & Mobile No.) |  |
| 12 | Nokia MSS Spoc  (Name, E-mail & Mobile No.) |  |
| 13 | Bharti NIAM Tool Spoc (Name, E-mail & Mobile No.) |  |
| 14 | Bharti Circle NWSO Spoc (Name, E-mail & Mobile No.) |  |
| 15 | MS Security Spoc  (Name, E-mail & Mobile No.) |  |
| 16 | Bharti Planning Team Spoc  (Name, E-mail & Mobile No.) |  |
| 17 | Bharti Central Security Team – Approved By  (Name, E-mail & Mobile No.) |  |

**Mandatory Security Controls:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 1 | User Access Management | Node shall support authentication and authorization mechanism and same shall be provisioned or enabled on all physical and virtual management connections. | |  |
| **Description** | | | **Audit Expectations** | |
| System access shall be enabled on the basis of username and with at least one authentication attribute e.g. password, certificate, keys etc.  Example of system access: -  1. App-based GUI (e.g. Thick Client / Java Applet).  2. Web-based GUI.  3. CLI (SSH and if any other mechanism).  4. Physical Console Login.  5. Other applicable interface e.g. SNMP, SFTP etc.  6. Operating system access. | | | Evidences with screenshots capturing system function access from all available interfaces e.g.,  1. App-based GUI (e.g. Thick Client / Java Applet).  2. Web-based GUI.  3. CLI (SSH and if any other mechanism).  4. Physical Console Login.  5. Other applicable interface e.g. SNMP, SFTP etc.  6. Operating system access. | |
| **OEM Comments:**  1. App-based GUI (e.g. Thick Client / Java Applet) == > Not applicable.  2. Web-based GUI. == > Not Applicable.  3. CLI (SSH and if any other mechanism). == > Applicable.  4. Physical Console Login. == > Not applicable.  5. Other applicable interface e.g. SNMP, SFTP etc. == > SFTP is applicable.  6. Operating system access. == > Applicable.  ===================================================================================================================  1. App-based GUI (e.g. Thick Client / Java Applet).  Not applicable  2. Web-based GUI ()  Applicable  3. CLI (SSH and if any other mechanism)    4. Physical Console Login.  Not applicable.  5. Other applicable interface e.g. SNMP, SFTP etc.  **SFTP :**    6.Operating system access.  OS access has been provided on user credential-based login | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 2 | User Access Management | Node shall have the capability to create unique user IDs along with associated privileges. There shall be mechanism to identify these users along with their privilege level. This is applicable for both OS and application level.  **Categorization of User in Airtel environment:**  - System internal (Built in user which are not accessible from user Interface).  - Generic User (Built in or on demand created user which is shared between people), for generic user suitable SOD will be required before creation.  - System Default (Built in user who password must be changed at the time of Handover).  - Machine to Machine User (User Created for establishing inter-machine communication only). NIAM users will be part of this list.  - End user (Human User) in case of glass break or NIAM outage situation these users will be used for Access. (This will cover Administrator users only). | |  |
| **Description** | | | **Audit Expectations** | |
| A unique user ID shall be created for all users (human user, machine to machine, application, or operating system) having access to the network element.  Users shall be identified as per their privilege level (roles/profile assigned).  User IDs created shall not give any indication of the user’s privilege level. For example, user ID shall not be created with names as admin, manager, supervisor, etc. | | | Evidence can be presented in the form of screenshot/screen-capture on showing list of all users configured on the system along with its privileges/roles assigned; (System screenshots/logs to be provided). | |
| **OEM Comments:**  **GUI (End user)**  **Please share user screen shoot from GUI. Share user justification in excel.** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**  **List of users to be amend in attached excel sheet.**       * **Artifact SS that no same name user can created.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 3 | User Access Management | Node shall have capability to display all active users in the system along with their last login date. | |  |
| **Description** | | | **Audit Expectations** | |
| The system shall publish details about user accounts including:  - All active users in the system.  - Last login details of the user.  This will facilitate administrator/system to take action from user management control perspective (e.g. disabling/deleting dormant accounts, etc.). | | | Evidence can be presented in the form of screenshot/screen-capture on showing a list of all users configured on the system along with its last login details. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**  **GUI :**  **Please share last login detail SS from GUI.**  **CLI :**   * **Users last login details.** | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | | | **Compliance Status (FC, NC, NA)** |
| 4 | User Access Management | Idle session timeout (Inactivity time-out period) shall be configured as 10 minutes for Human / Generic user account. | | | |  |
| **Description** | | | | **Audit Expectations** | | |
| An OAM user interactive session shall be locked-out automatically after a specified period of inactivity i.e. 10 minutes.  **Note:** Timeout must cover all login session (e.g. sessions accessed via terminal or web portal along with physical access to ports). | | | | Evidence can be presented in the form of screenshot/screen-capture on showing in-built system configuration of Idle sessions time-out.  Evidence must cover all login session for Human / Generic User accounts e.g. sessions accessed via terminal or web portal along with physical access to ports. | | |
| **OEM Comments:**  **Web-GUI**  Please share timeout configuration and artifact SS from GUI. | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Timeout configuration SS.**      * **Timeout artifact SS.** | | | | | | |
| **S. No.** | **Category** | | **Control** | | | **Compliance Status (FC, NC, NA)** |
| 5 | User Access Management | | Node shall not disclose system information along with user details. System shall not provide information about which part of the authentication is incorrect. | | |  |
| **Description** | | | | | **Audit Expectations** | |
| Logon failure messages shall not disclose information about the system and user details, if wrong username or password is entered no information to the user other than invalid attempt shall be displayed.  **Note:** This is applicable across all login access e.g. SSH, RDP, Console, SFTP, GUI etc. | | | | | Evidence can be presented in the form of screenshot/screen-capturing failed login attempts on the system. Failed login attempt needs to be performed in following manner:  1. Username is correct, but password is incorrect.  2. Username is incorrect with random password. | |
| **OEM Comments:**  **GUI**  Need to share below SS from GUI.   1. Username is correct, but password is incorrect. 2. Username is incorrect with random password. | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Username is correct but password incorrect.**      * **Username is incorrect but password is correct.** | | | | | | |
| **S. No.** | **Category** | **Control** | | | | **Compliance Status (FC, NC, NA)** |
| 6 | User Access Management | Node shall be configured with account lockout policy; it must delay login by 30 minutes after 6 failed login attempts. | | | |  |
| **Description** | | | | **Audit Expectations** | | |
| The maximum permissible number of consecutive failed user account login attempts must be configured by system and there should be a block delay in allowing the user to attempt login again.  Once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.  As per BISP policy; it must delay login by 30 minutes after 6 failed login attempts.  **Note:** Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.). | | | | Evidence can be presented in the form of screenshot/screen-capture on executing following steps:  1) Perform consecutive failed login attempts for the user account until the default maximum number of preconditions is reached.  2) Attempt again one extra login, which fails again.  3) Attempt one extra login in less time than the default for the delay, using the correct credentials.  4) Attempt one extra login in more time than the default for the delay, using the correct credentials. | | |
| **OEM Comments:**  **GUI**  **Please share below SS for GUI also.** | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Configuration SS.**        * **6 fail login SS.**      * **After 6 fail login user lock SS.**      * **After 20 min try to login with correct passowrd but user is locked.**      * **After 30 min user login successfully.** | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S. No.** | **Category** | | **Control** | | | | | **Compliance Status (FC, NC, NA)** |
| 7 | User Access Management | | All the users which are created during project phase must be deleted at the time of handover. All the system Internal / machine to machine / system default user password must be reset and then shared with MS team. | | | | |  |
| **Description** | | | | | **Audit Expectations** | | | |
| All pre-configured accounts during project phase along with predefined / default / factory accounts shall be deleted or disabled.  1. Deleting user account created during project phase will ensure that only specific defined accounts can access resources on the system going ahead in production environment.  2. Default user IDs which cannot be deleted such as root, admin, for such users, password shall be changed upon installation (before production deployment). The new password set must be selected as per complexity defined in BISP policy.  Note: Above requirements shall be applicable for passwords used for all users in the system (e.g. application-level, OS-level, etc.). | | | | | 1. Evidence can be presented in the form of screenshot/screen-capture on showing list of all users configured on the system along with its privileges/roles assigned; (System screenshots/logs to be provided)  2. List of accounts configuration during projects phase and its removal evidences (Screenshots).  3. List of accounts created along with its usage details (requirement for what purpose accounts are created on the system) required as mentioned below;  a. Account name  b. Roles/Profiles assigned  c. Usage details (requirements for which user created)  d. Applicable interface access e.g. CLI, GUI etc.  e. Categorization of User from below section  - System internal (Built in user which are not accessible from user Interface)  - Generic User (Built in or on demand created user which is shared between people), for generic user suitable SOD will be required before creation.  - System Default (Built in user who password must be changed at the time of Handover)  - Machine to Machine User (User Created for establishing inter-machine communication only). NIAM users will be part of this list.  - End user (Human User) in case of glass break or NIAM outage situation these users will be used for Access. (This will cover Administrator users only).  4. Evidence can be presented in the form of screenshot/screen-capture on showing password changed for all default accounts (which must have information/display stating that password is changed) through manual configuration.  Note: OEM to provide list of all predefined accounts documented in their Operational/Support Manual for verification/audit purpose. Instructions of how administrator user can view all existing accounts in the database are provided in the documentation accompanying the network element. | | | |
| **OEM Comments:**  **List of GUI Based Users**  **Please share user SS from GUI** | | | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Need to attach mail from Infra side that all test user is deleted, and password has been changed.** * Artifact that all test user has been deleted. | | | | | | | | |
| **S. No.** | | **Category** | | **Control** | | | **Compliance Status (FC, NC, NA)** | |
| 8 | | User Access Management | | Node must be integrated with NIAM before the MS handover. | | |  | |
| **Description** | | | | | | **Audit Expectations** | | |
| NIAM solution is implemented in Airtel environment to ensure centralized access (authentication/authorization) mechanism. Centralized access control management provide ease of administration/monitoring across the network.  Adequate access-control to be implemented to ensure that node is only accessible from NIAM. | | | | | | Evidence stating that node is successfully integrated with NIAM server and respective roles/users configured as per NIAM requirements | | |
| **OEM Comments:** | | | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Need to attach mail from NIAM team that node is integrated with NIAM.** | | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 9 | User Access Management | The user profile at the node level shall be configured as per NIAM integration requirement i.e. Read Only, Read / Write, Administrator. | |  |
| **Description** | | | **Audit Expectations** | |
| Each node must have minimum of three user profiles for NIAM, e.g.,  **1. Read Only**  i) No modifying and execution capability  **2. Read / Write**  i) No access right for user creation, modification and deletion  ii) No access right for deletion, modification, disabling and altering of logs etc.  iii) No access to CDR / IPDR logs  iv) No access to Lawful interception commands  **3. Administrator**  If the node is having more than three user profiles other than (Read Only, Read/Write, Administrator); then against each profile there must be a user for NIAM access so that specific demand related to other profile can be handled from NIAM. | | | 1. Evidence can be presented in the form of screenshot/screen-capture on showing list of all users configured on the system along with its privileges/roles assigned; (System screenshots/logs to be provided)  2. List of accounts configuration during projects phase and its removal evidences (Screenshots).  3. List of accounts created along with its usage details (requirement for what purpose accounts are created on the system) required as mentioned below;  a. Account name  b. Roles/Profiles assigned  c. Usage details (requirements for which user created)  d. Applicable interface access e.g. CLI, GUI etc.  e. Categorization of User from below section  - System internal (Built in user which are not accessible from user Interface)  - Generic User (Built in or on demand created user which is shared between people), for generic user suitable SOD will be required before creation.  - System Default (Built in user who password must be changed at the time of Handover)  - Machine to Machine User (User Created for establishing inter-machine communication only). NIAM users will be part of this list.  - End user (Human User) in case of glass break or NIAM outage situation these users will be used for Access. (This will cover Administrator users only). | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**     * **Artifacts that NIAM RW user does not fire critical command.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 10 | User Access Management | All mode of node access (CLI, GUI, WEB etc.) shall have separate users for NIAM integration and same shall be provisioned. | |  |
| **Description** | | | **Audit Expectations** | |
| It is advised that all the access mechanisms are identified and integrated with NIAM setup to avoid any misuse through uncontrolled access mechanism. The user profile at the node level must be configured as per NIAM integration requirement for each access medium i.e., CLI, GUI/WEB, etc. | | | 1. Evidence can be presented in the form of screenshot/screen-capture on showing list of all users configured on the system along with its privileges/roles assigned; (System screenshots/logs to be provided).  2. List of accounts created along with its usage details (requirement for what purpose accounts are created on the system) required as mentioned below:  a. Account name  b. Roles/Profiles assigned  c. Usage details (requirements for which user created)  d. Applicable interface access e.g. CLI, GUI etc.  e. Categorization of User from below section  - System internal (Built in user which are not accessible from user Interface).  - Generic User (Built in or on demand created user which is shared between people), for generic user suitable SOD will be required before creation.  - System Default (Built in user who password must be changed at the time of Handover).  - Machine to Machine User (User Created for establishing inter-machine communication only). NIAM users will be part of this list.  - End user (Human User) in case of glass break or NIAM outage situation these users will be used for Access. (This will cover Administrator users only). | |
| **OEM Comments:**  **GUI Based login** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Need to attach mail from NIAM team that nodes are integrated with NIAM.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 11 | Password Management | Node shall be configurable with password complexity policy; following requirements shall be configured:  Minimum password length should be:  1. 8 characters or greater for Human user accounts. | |  |
| **Description** | | | **Audit Expectations** | |
| Password complexity feature must be enforced as per BISP policy by system across all accounts/password when they are configured or changed.  **Note 1:** If NIAM (central system) is used for user authentication, then password policy must be applicable for central system and additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system.  **Note 2:** Above requirements shall be applicable for all passwords used in system (e.g. application-level, OS-level, etc.). | | | 1. Evidence can be presented in the form of screenshot/screen-capture on showcasing current password complexity feature enabled on the system.  2. Evidences can be presented where user tries configuring the same password as it is of user-id with respective alert messages generated. | |
| **OEM Comments:**  **GUI Based**  **Please share password length configuration and artifact SS for GUI also** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Password complexity configuration SS.**        * **Error SS when user set 7 digit password.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 12 | Password Management | Node shall be configurable with password complexity policy; following requirements shall be configured:  Minimum password length should be 16 characters or greater for machine accounts wherever system supports else it should be minimum 8 characters. | |  |
| **Description** | | | **Audit Expectations** | |
| Password complexity feature must be enforced as per BISP policy by system across all accounts/password when they are configured or changed.  Note 1: If NIAM (central system) is used for user authentication, then password policy must be applicable for central system and additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system.  Note 2: Above requirements shall be applicable for all passwords used in system (e.g. application-level, OS-level, etc.). | | | 1. Evidence can be presented in the form of screenshot/screen-capture on showcasing current password complexity feature enabled on the system.  2. Evidences can be presented where user tries configuring the same password as it is of user-id with respective alert messages generated. | |
| **OEM Comments:**  **GUI Based**  **Please share password length configuration and artifact SS for GUI also** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **SS for NIAM User password is 8 char.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 13 | Password Management | Node shall be configurable with password complexity policy; following requirements shall be configured for all type of users in the system.  Password complexity should be enabled to ensure it comprises of at least three of the following categories:  - at least 1 uppercase character (A-Z).  - at least 1 lowercase character (a-z).  - at least 1 digit (0-9).  - at least 1 special character (e.g., @ ; ! $ .). | |  |
| **Description** | | | **Audit Expectations** | |
| Password complexity feature must be enforced as per BISP policy by system across all accounts/password when they are configured or changed.  **Note 1:** If NIAM (central system) is used for user authentication, then password policy must be applicable for central system and additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system.  **Note 2:** Above requirements shall be applicable for all passwords used in system (e.g. application-level, OS-level, etc.). | | | 1. Evidence can be presented in the form of screenshot/screen-capture on showcasing current password complexity feature enabled on the system.  2. Evidences can be presented where user tries configuring the same password as it is of user-id with respective alert messages generated. | |
| **OEM Comments:**  **GUI:**  **Please share password complexity configuration and artifact SS from GUI** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Password complexity configuration SS.**     **Testing Screenshots.**   * **Removed digit.**      * **Removed Upper case.**      * **Removed Lower case.**      * **Removed Special char.** | | | | |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S. No.** | | **Category** | **Control** | | | | **Compliance Status (FC, NC, NA)** | | |
| 14 | | Password Management | Node shall be configurable with password complexity policy; following requirements shall be configured:  Password shall not contain initial 4 characters of the user account name. | | | |  | | |
| **Description** | | | | | | **Audit Expectations** | | | |
| Password complexity feature must be enforced as per BISP policy by system across all accounts/password when they are configured or changed.  **Note 1:** If NIAM (central system) is used for user authentication, then password policy must be applicable for central system and additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system.  **Note 2:** Above requirements shall be applicable for all passwords used in system (e.g. application-level, OS-level, etc.). | | | | | | 1. Evidence can be presented in the form of screenshot/screen-capture on showcasing current password complexity feature enabled on the system.  2. Evidences can be presented where user tries configuring the same password as it is of user-id with respective alert messages generated. | | | |
| **OEM Comments:** | | | | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Configuration SS.**      * **Error when user set password which has first 4 char same as username.** | | | | | | | | | |
| **````````````** | **Category** | | | **Control** | | | | **Compliance Status (FC, NC, NA)** |
| 15 | Password Management | | | BIOS shall have login-password enabled (Not boot password). | | | |  |
| **Description** | | | | | **Audit Expectations** | | | |
| System BIOS or UEFI firmware must be protected by password that meets password complexity requirements as per BISP policy in order to:  1. Restrict people from booting the system from removable devices.  2. Changing BIOS or UEFI settings without permission. | | | | | Evidence can be presented in the form of screenshot/screen-capture of system setting ensuring BIOS login-password is enabled.  Also, team can submit the reboot procedure where BIOS login-password is required as input. | | | |
| **OEM Comments:** | | | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Need to attach SS that BIOS is encrypted with password.** | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S. No.** | | **Category** | | **Control** | | | **Compliance Status (FC, NC, NA)** | |
| 16 | | Password Management | | Node shall be configurable with password age policy; it shall meet below criteria:  1. Maximum password age must be 90 days or less. | | |  | |
| **Description** | | | | | **Audit Expectations** | | | |
| Password age feature shall be in place to determine the period of time (in days) that a password can be used before the system requires the user to change it.  Note: Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.). An exception to this requirement are accounts such as internal or system accounts. | | | | | Evidence can be presented in the form of screenshot/screen-capture of password policy implemented in the system. | | | |
| **OEM Comments:**  **GUI:**  **Please share password age configuration and artifact SS from GUI.** | | | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Configuration SS.**      * **Artifact SS.** | | | | | | | | |
| **S. No.** | **Category** | | **Control** | | | | | **Compliance Status (FC, NC, NA)** |
| 17 | Password Management | | Machine to Machine password age shall be of 180 days. Wherever, certification-based authentication is feasible between nodes, same needs to be implemented. | | | | |  |
| **Description** | | | | | | **Audit Expectations** | | |
| This control is applicable for Machine account. The password age setting shall be in place to determine the period of time (in days) that a password can be used before the system requires the user to change it.  **Note:** Machine Accounts are the accounts which will be used for authentication and authorization from machine to machine or between applications on nodes and cannot be assigned to a single person or a group of persons. | | | | | | Evidence can be presented in the form of screenshot/screen-capture of password policy implemented in the system. | | |
| **OEM Comments:**  **GUI:**  **Please share password age configuration and artifact SS from GUI.** | | | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Machine to Machine user password age SS.** | | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 18 | Password Management | Node shall be configurable to ask for old password at the time changing password. | |  |
| **Description** | | | **Audit Expectations** | |
| Users shall be permitted to change their passwords only if they have been properly authenticated to the system by entering old password at the time, they make the request of password change. | | | Evidence can be presented in the form of screenshot/screen-capture on how the system prompts for old password while password reset. | |
| **OEM Comments:**  **GUI:**  **Please share artifact SS from GUI that when user want to change password he need to put old password first.** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Artifact SS when user want to change password he need to put old password first.** | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S. No.** | **Category** | | **Control** | | | **Compliance Status (FC, NC, NA)** |
| 19 | Password Management | | Node shall be configurable to change their password after first initial login. | | |  |
| **Description** | | | | **Audit Expectations** | | |
| Node must be configured to force the users to change the initial password immediately after the first logon. | | | | Evidence can be presented in the form of screenshot/screen-capture on how the system prompts for password change at first logon. | | |
| **OEM Comments:**  **GUI:**  **Please share configuration and artifact SS from GUI also.** | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Configuration SS for first login password must change.**      * **Artifact SS.** | | | | | | |
| **S. No.** | **Category** | **Control** | | | | **Compliance Status (FC, NC, NA)** |
| 20 | Password Management | Password history shall be maintained, it shall disallow last 4 number (or more) of previously used passwords. | | | |  |
| **Description** | | | | | **Audit Expectations** | |
| Node shall enforce password history policy setting which determines the number of unique new passwords that must be associated with a user account before an old password can be reused. | | | | | Evidence can be presented in the form of screenshot/screen-capture of password policy implemented in the system. | |
| **OEM Comments:**  **GUI:**  **Please share configuration and artifact SS from GUI also.** | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Configuration SS.**      * **Error SS when tried same password.** | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 21 | Password Management | Passwords shall be protected with strong cryptography during storage. | |  |
| **Description** | | | **Audit Expectations** | |
| Password shall be saved / stored with one-way hash algorithm and not in plain text format. The preferred hash function is SHA-512. It is also recommended that using a randomly generated salt for every password. This will make breaking insignificantly more difficult. | | | Evidence can be presented in the form of screenshot/screen-capture of all records comply with the characteristic of one-way hash result.  Considering the criticality of information; it is advised that manual testing/verification is performed. OEM can submit the adequate documents to prove the compliance against this controls. | |
| **OEM Comments:**  **GUI:**  **Please share configuration and artifact SS from GUI also.** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Configuration SS.**      * **Artifact SS.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 22 | System Hardening | Node shall be hardened as per supplier hardening guidelines. | |  |
| **Description** | | | **Audit Expectations** | |
| Partner / OEM shall have provisions to ensure that the equipment / services / software they supply are “safe to connect” in the network.  As per DoT requirements, it is necessary to ensure that node which are getting inducted in network should be tested with respect to network security.  DoT security test report should be submitted for validation. | | | 1. Node documentation containing information about complete solution/system details (and its internal components) along operational and security manual shall be provided by OEM.  2. OEM shall submit the security testing certificate of node which got tested from any international agency/labs of the standards e.g. Common Criteria Labs in case of ISO/IEC 15408 standards.  3. OEM shall provide detailed security assessment report of the testing performed along with the results and mitigation plans of open observations. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Need approval mail from Deepak Sethi Sir or Deepak Pandey Sir.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 23 | System Hardening | No unlicensed / freeware / shareware / demo software must be installed.  Unnecessary utilities (software and hardware) shall be disabled from node during commissioning. | |  |
| **Description** | | | **Audit Expectations** | |
| OEM shall ensure that at the time of product development all such software which are unlicensed, freeware, shareware or demo version software must not be utilized and must not be installed during the node implementation in production network.  Unnecessary/unused utilities software components or parts of software (e.g. default web pages, example databases files, test data) which are not needed for operation or functionality of the node shall not be installed or shall be deleted after installation. | | | 1. OEM shall provide a list of all available software and libraries and associated components containing at least the following information shall be included in the documentation accompanying the network element:  - name of the software / library;  - version of the software / library installed;  - list of dependencies and versions;  - any add-ons and functions;  - any special hardware/debugging ports;  - software support type;  - licensing information;  - brief description of their purpose.  2. Team should provide the details about software /libraries or components which are installed in the system using any suitable command line tools or any other suitable means of determination.  3. Validation required with justification that there are no entries in the list of software / libraries installed in the system apart from the ones that have been mentioned and deemed necessary for the operation of the network element in the attached documentation. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **RHEL Version.**      * **RPM package list.**      * **Need to attach SS of s/w package in product doc and ISO/IEC 15408 standards certification of application.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 24 | System Hardening | OEM shall share the communication matrix (list of all listening ports required as per product document).  No unnecessary or unwanted port should be open other than required by the product.  Highlight which all ports can be configured to work on non-default ports (if any) and has been tested in lab or on field. | |  |
| **Description** | | | **Audit Expectations** | |
| Node runs with required services / ports to ensure adequate communication with its peer nodes as per functionality of node.  Port matrix must have all required information as mentioned below:  1. Port Number.  2. Service/Protocol tagged with Port Number.  3. Service information in details (Protocol details).  4. Peer node information.  5. Purpose/Usage details. | | | 1. OEM to share the operational manuals along with reference to communication matrix stating the service/port details as per below section:  Port matrix should have all required information as mentioned below:  1. Port Number.  2. Service/Protocol tagged with Port Number.  3. Service information in details (Protocol details).  4. Peer node information.  5. Purpose/Usage details.  2. OEM to share the node level services running along with its applicable ports enabled on the system e.g. netstat output detailing above requirements. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Open port SS.**      * **Need VA approval mail.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 25 | System Hardening | All external drives like floppy drives, CD/DVD/Blu-ray ROM & USB shall be disabled on all node. | |  |
| **Description** | | | **Audit Expectations** | |
| Disable USB / CD-DVD / Floppy port access on the device. In case USB / media ports are active, there is a risk that any user having physical access to the node may insert a device with malicious content. This may further result in the installation of an application or a malicious program (malware, virus, etc.) on the node. | | | Evidence can be presented in the form of screenshot/screen-capture of following information.  1. List of available interfaces/ports for Floppy drives, CD/DVD/Blu-ray ROM & USB access.  2. Its current status (enabled/disabled). | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **No USB Storage attached.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 26 | System Hardening | Node shall be integrated with authorized NTP Server. | |  |
| **Description** | | | **Audit Expectations** | |
| Node shall be synchronized with primary and secondary NTP source / servers. | | | 1. Evidence can be presented in the form of screenshot/screen-capture of IP reachability to/from NTP server. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 27 | System Hardening | Node shall be integrated with SNMPv3 to provides secure access to devices by authenticating and encrypting data packets over the network. | |  |
| **Description** | | | **Audit Expectations** | |
| Enable SNMP v3 with security level set to authPriv. | | | 1. Evidence can be presented in the form of screenshot/screen-capture of SNMP servers in the network.  2. Evidence of security level configured on SNMP. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **SNMP service SS.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 28 | System Hardening | All operating system, applications and firmware shall be updated with latest stable patch. Anti-virus shall be regularly updated with latest signature. | |  |
| **Description** | | | **Audit Expectations** | |
| The system must be updated to the latest version including patches and bug fixes for both operating system and application. The vendor shall also share the patch / version release document. | | | 1. Evidence can be presented in the form of screenshot/screen-capture of latest system patches / version installed on node. | |
| **OEM Comments:**  **GUI:**  **Artifact SS that all application plugins are updated.** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**  **Please share SS against below points. All firmware and OS version must be updated.**   * **Firmware version of ethernet port.** * **Firmware version of HBA card.** * **System BIOS version.** * **Firmware version of tape device st0.** * **Firmware version id SMART array controllers.** * **Firmware version of installed applications.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 29 | Log Management | Node shall be able to generate all command logs (including authentication, password reset and other activities). | |  |
| **Description** | | | **Audit Expectations** | |
| Enforce command logging to detect and capture evidence for analysis of the events.  Command logging must be enabled to capture details such as:  - user name or user id (WHO).  - timestamp (WHEN).  - source IP address (FROM WHERE).  - command fired (WHAT).  - Node name/ID. | | | 1. The following information shall be provided by OEM as part of the documentation accompanying the network element:  - The log where the event is recorded and how it can be accessed (e.g. the complete path).  - List of events/logs types are defined to capture the event/incidents.  - If the event type is enabled by default or how to enable it.  2. Evidence can be presented in the form of screenshot/screen-capture of log files/folders with sample data to validate whether logs are capturing all required information or not. | |
| **OEM Comments:**  **GUI**  **Please share log SS form GUI.** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Artifact SS.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 30 | Log Management | All command logs must be transferred to A-log server for DoT compliance on SFTP protocol. | |  |
| **Description** | | | **Audit Expectations** | |
| To meet DoT requirements, all command logs must be transferred to A-log server.  An external centralized syslog server must be in place for storing logs as per DoT requirements i.e. 1 year online and further 2 year offline.  **Note:** Transfer of logs must be secured using an encrypted channel. | | | 1. Evidence can be presented in the form of screenshot/screen-capture of IP reachability to/from A-log server.  2. Evidence stating that node is successfully integrated with A-log server and transfer/storage of logs initiated. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Need to share NWSO approval mail.** | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | | | **Compliance Status (FC, NC, NA)** |
| 31 | Log Management | Node shall be able to generate all event Logs {username, timestamp, performed action, result, length of session, interface, resource usage (values exceeded and/or value reached) etc.,} and same shall be enabled.  Complete log path defined on the node shall be shared. | | | |  |
| **Description** | | | | | **Audit Expectations** | |
| Logging of security events must be enabled to ensure that important system messages and diagnostic information is recorded for both application and operating system. (i.e., Access logs, Command logs, Security logs, System logs etc.).  Following are the events that should be logged as per 3GPP TS 33.117 V16.1.0 (2019-03) guidelines:  1. Incorrect login attempts  (Records any user incorrect login attempts to the system)  2. Administrator access  (Records any access attempts to accounts that have system privileges)  3. Account administration  (Records all account administration activity, i.e. configure, delete, enable, and disable)  4. Resource Usage  (Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds)  5. Configuration change  (Changes to configuration of the system)  6. Reboot / shutdown / crash  (This event records any action on the system that forces a reboot or shutdown)  7. Interface status change  (Change to the status of interfaces on the network device (e.g. shutdown))  8. Change of group membership or accounts  (Any change of group membership for accounts) | | | | | 1. The following information shall be provided by OEM as part of the documentation accompanying the network element:  - The log where the event is recorded and how it can be accessed (e.g. the complete path).  - List of events/logs types are defined to capture the event/incidents  - If the event type is enabled by default or how to enable it.  2. Evidence can be presented in the form of screenshot/screen-capture of log files/folders with sample data to validate whether logs are capturing all required information or not. | |
| **OEM Comments:**  Application logs evidence pending with Nokia MSS | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Access logs.**      * **Change logs.**      * **Need to attach confirmation mail from SOC Team.** | | | | | | |
| **S. No.** | **Category** | | **Control** | | | **Compliance Status (FC, NC, NA)** |
| 32 | Log Management | | All Logs / Events / Alarms generated in the node shall be transferred to SIEM / SOC solutions on syslog or other means available on the node. | | |  |
| **Description** | | | | **Audit Expectations** | | |
| Security events and system alarms generated by the node must be forwarded in real-time to a central analytics platform (e.g. SIEM). The analysis of logged entries must be automated and aggregated with correlation rules.  It is recommended that node is integrated with SIEM/SOC infrastructure for automated monitoring of logs to detect security events in run time.  **Note 1:** The system administrator must be alerted with all type of mis-functioning. None of the alarms shall be blocked.  **Note 2:** Alarms must be configured for all types of events. | | | | 1. Evidence can be presented in the form of screenshot/screen-capture of IP reachability from SOC/SIEM setup (Ping response).  2. Evidence stating that node is successfully integrated with SOC/SIEM and monitoring of logs initiated (configuration performed at node level for SIEM integration). | | |
| **OEM Comments:**  **GUI Logs** | | | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Need to attach confirmation mail from SOC Team.** | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 33 | Log Management | The audit log shall be protected from unauthorized access or destruction by means of access controls based on user privileges. | |  |
| **Description** | | | **Audit Expectations** | |
| Security event logs shall be access controlled (file access rights) so only privilege users have access to the log files.  Set strict permissions on all log file/folders with read only permission (so that it is not modified).  **Note:** Log should be protected with file access restriction at system as well as at centralized log server. It shall not be modified to maintain the integrity of log data. | | | 1. OEM shall provide documentation describing where logs are stored (e.g. the complete path) and how these logs are accessed (privileges and interfaces).  2. Evidence can be presented in the form of screenshot/screen-capture of file/folder permission of location where logs are stored. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Artifacts that RO and RW user unable to access audit log.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 34 | Log Management | The security administrator shall be immediately notified if the audit log fails to record the events that are required to be recorded. | |  |
| **Description** | | | **Audit Expectations** | |
| System must ensure that logs are getting generated to capture critical information, in case of failure sufficient mechanism must be in place to take appropriate action.  SIEM / SOC infrastructure must be implemented to monitor / process logs to detect security events in run time. | | | The following information shall be provided by OEM as part of the documentation accompanying the network element:  - The log where the event is recorded and how it can be accessed (e.g. the complete path).  - List of events/logs types are defined to capture the event/incidents.  - If the event type is enabled by default or how to enable it.  - List of existing features through which the system administrator alerted with all type of mis-functioning. None of the alarms shall be blocked.  - List of events configured and enabled on the system which ensure that alerts generated in case of audit log failure. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Log configuration SS.**      * **Need to attach confirmation mail from SOC Team.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 35 | Communication Security | Secure Management Interface protocol / service shall be used to access system over O&M interface.  Insecure services and protocols must be deactivated. | |  |
| **Description** | | | **Audit Expectations** | |
| Communication link for management plane connectivity must be protected by cryptographically secure protocols.  Protocol Example: Use of SFTP instead FTP, HTTPS instead HTTP, SSH instead of Telnet, Secure RDP etc. must be in place.  Only secure services required for operational need of the system must be enabled and others must be deactivated.  Followings are few examples of services which must be disabled on the node.  1. FTP (File transfer protocol)  2. TELNET  3. TFTP (Trivial File Transfer Protocol)  4. RLOGIN (Remote login)  5. RSH (Remote shell)  6. RCP (Remote copy)  7. HTTP (Hypertext Transfer Protocol)  8. SNMP v1, v2 (Simple Network Management Protocol)  9. BOOTPS (Bootstrap Protocol)  10. Discovery protocols (CDP, LLDP)  11. IP Identification Service (Identd)  12. PAD (Packet assembler/disassembler)  13. MOP (Maintenance Operation Protocol)  14. SSHv1 (Secure Shell)  15. TCP/UDP Small Servers (Echo, Chargen, Discard und Daytime)  16. SMBD and NMBD (Server Message Block and NetBIOS)  17. NFS (Network File System)  18. REXEC (Remote exec)  19. Autofs (Automount)  20. PORTMAP (Portmapper)  21. RSTATD (Performance statistics)  22. RWALLD (Remote Write All Daemon)  23. DTSPCD (CDE Subprocess Control Service daemon)  24. RSYNC (Remote synchronization)  25. DHCPD (Dynamic Host Configuration Protocol)  26. TTDBSERVER (ToolTalk database server)  27. ECHO  28. DISCARD  29. SYSTAT  30. SPRAYD  31. SENDMAIL  32. CHARGEN  33. RUSERS  34. WHOIS  35. Finger | | | 1. Evidence can be presented in the form of screenshot/screen-capture of running services/application on the system.  2. Output of network services along with process running on the system should be shared e.g., Netstat and psinfo, etc.  3. List of O&M interfaces and its corresponding protocol information to be provided. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Open port SS.**      * **Need to attach VA confirmation mail.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 36 | Communication Security | Disable transmission of ICMP redirect and unreachable (ICMP) packet, if not required. | |  |
| **Description** | | | **Audit Expectations** | |
| Few flags in ICMP represent a risk to the node or network. (For ex. Ping of Death attack). Such flags should be disabled or filtered and not be answered, send or processed by the node.  The following ICMP types / flags should not be responded to or processed under any circumstances.  1. Redirect.  2. Unreachable packet. | | | 1. Evidence can be presented in the form of screenshot/screen-capture of ICMP redirect and unreachable configuration.  2. Evidence can be presented in the form of screenshot/screen-capture of iptables if it is configured. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **NA** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 37 | Security Assessment | Reachability must be established with centralized vulnerability scanner as part of Integration. Node must be scanned for vulnerabilities by security team. | |  |
| **Description** | | | **Audit Expectations** | |
| Vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from Airtel's security policy. This is done by identifying the operating systems and major software applications running on the hosts and matching them with information on known vulnerabilities stored in the scanners’ vulnerability databases.  Ensure that node is reachable from vulnerability assessment scanner.  Node must be scanned for vulnerabilities by security team before go-live. | | | 1. Evidence can be presented in the form of screenshot/screen-capture of IP reachability from Vulnerability assessment scanner (Ping response).  2. Submit VA reports generated by scanner. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Need to attach VA mail that Node reachable from scanners.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 38 | Security Assessment | All critical and high vulnerabilities must be closed by OEM and on the declaration of OEM's closure of VA report; a fresh scan will be conducted by security team. Based on the fresh scan report if all critical and high vulnerabilities are closed then only the control will be declared compliant.  Software restrictions should be used to restrict malicious code execution. | |  |
| **Description** | | | **Audit Expectations** | |
| OEM must address all high/critical observations before go-live.  Rescan is mandatory to ensure that critical and high vulnerabilities are addressed adequately. | | | 1. Initial and Re-test vulnerability assessment report.  2. Evidences on closure of critical/high vulnerabilities identified. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **All Vulnerabilities are addressed as per the Quarterly VA scan process and SoD being provided wherever necessary. ( Need to attach VA confirmation mail)** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 39 | Security Assessment | Mitigation plan for Medium and Low vulnerabilities shall be provided. | |  |
| **Description** | | | **Audit Expectations** | |
| OEM must share plan for all medium/low observations before go-live. | | | 1. Initial and Re-test vulnerability assessment report.  2. Evidences on closure of medium/low vulnerabilities identified. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **VA scan is performed, and vulnerabilities are addressed before RTP Go Live. ( Need to attach VA confirmation mail )** * **Share mitigation plan of vulnerabilities.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 40 | Security Assessment | Configuration backup integrity check shall be present as a build in design on node. | |  |
| **Description** | | | **Audit Expectations** | |
| Backup and restoration procedures shall be established and implemented to ensure the integrity and availability of critical information. When backup is being performed, it is mandatory to consider integrity of backup media. Backup should not be allowed to restore in case of integrity violation.  OEM shall certify that integrity backup design is built in feature on node. | | | 1. Evidence can be presented in the form of screenshot/screen-capture of backup service / application and check for backup integrity on the system along with backup process. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Show Backup integration is in place.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 41 | Documentation | Product manual for nodes shall be present and available with OEM and shared with Airtel. | |  |
| **Description** | | | **Audit Expectations** | |
| Product manuals should be readily available to Airtel such as operational manual, security manual, hardening guides for nodes provided by OEM. | | | 1. Evidence can be provided that product manual documents of OEM are readily available with Airtel. | |
| **OEM Comments:**  update | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Attached confirmation mail from Deepak Sethi Sir or Deepak Pandey Sir for product doc and all other doc.** | | | | |

**Good to have security controls:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 1 | User Access Management | A legal banner shall be displayed to provide adequate protection and awareness of legal issues. | |  |
| **Description** | | | **Audit Expectations** | |
| An appropriate login message must be displayed to the user when he/she tries to login to the system. This file must contain warnings about inappropriate and unauthorized use of the system.  Configure below legal warning banner on the login page of the system:  ***This system belongs to Airtel. All content on this system is confidential in nature. The activities to this system may be monitored, recorded, or captured in order to comply with Airtel internal policies. Any unauthorized use of the system or the information therein shall be subjected to disciplinary action and may lead to criminal prosecution. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.***  **Note:** Legal warning banner to be configured for all login access type e.g. Local console, remote console, web etc. | | | Evidence can be presented in the form of screenshot/screen-capturing banner displayed at the time of system login. | |
| **OEM Comments:**  **GUI:**  **Please share GUI SS also.** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Artifact SS.** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **Category** | **Control** | | **Compliance Status (FC, NC, NA)** |
| 2 | Password Management | Node shall be configurable with password age policy; it shall meet below criteria:  1. Minimum password age should be 7 days or more. | |  |
| **Description** | | | **Audit Expectations** | |
| Password age feature shall be in place to determine the period of time (in days) that a password can be used before the system requires the user to change it.  Note: Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.). An exception to these requirements are accounts such as internal or system accounts. | | | Evidence can be presented in the form of screenshot/screen-capture of password policy implemented in the system. | |
| **OEM Comments:** | | | | |
| **MS OPS /MS SECURITY SPOC Comments:**   * **Minimum password age artifact.** | | | | |