# *Special Access Policy*

## *Version 2.6*

# Document version control page
# Prepared By

| Version | Date | Author | Update Description |
|---|---|---|---|
| 1.0 | 12/06/08 | JayaseelanJ | Initial Issue |
| 1.1 | 22/08/08 | JayaseelanJ | Format changes |
| 1.2 | 10/09/09 | JayaseelanJ | Policy Document Reviewed |
| 1.3 | 12/07/2010 | J.Jayaseelan | Policy Document Reviewed |
| 1.4 | 25/11/2011 | Jayaseelan J | Policy Document Reviewed and ISM Name changed to ISH |
| 1.5 | 27/06/2012 | Jayaseelan J | Policy Document Reviewed |
| 1.6 | 27/06/2013 | Jayaseelan J | Policy Document Reviewed |
| 1.7 | 21/06/2014 | Jayaseelan J | Policy Document Reviewed |
| 1.8 | 01/08/2014 | Jayaseelan J | Policy Document Reviewed as per ISO 27001:2013 requirement |
| 1.9 | 22/06/2015 | Jayaseelan J | Policy Document Reviewed |
| 2.0 | 14/06/2016 | Jayaseelan J | Policy Document Reviewed |
| 2.1 | 15/11/2017 | Santhosh S | Policy Document Reviewed |
| 2.2 | 12/06/2018 | Santhosh S | Policy Document Reviewed |
| 2.3 | 10/07/2019 | Santhosh S | Policy Document Reviewed |
| 2.4 | 09/11/2020 | Santhosh S | Policy Document Reviewed |
| 2.5 | 06/12/2021 | Santhosh S | Policy Document Reviewed |
| 2.6 | 02/12/2022 | Santhosh S | Policy Document Reviewed |

# Reviewed and Approved By

| Version | Date | Reviewed by | Approved By | Owner |
|---|---|---|---|---|
| 1.0 | 12/06/08 | Mr. Madhavaswamy | Mr. R.Kumar | ISM |
| 1.1 | 22/08/08 | Mr. Madhavaswamy | Mr. R.Kumar | ISM |
| 1.2 | 10/09/09 | HR Director | Mr. R.Kumar | ISM |

| | | | | |
|---|---|---|---|---|
| 1.3 | 13/07/2010 | HR Director | Mr. R.Kumar | ISM |
| 1.4 | 28/11/2011 | HR Director | Mr. R.Kumar | ISH |
| 1.5 | 27/06/2012 | HR Director | Mr. R.Kumar | ISH |
| 1.6 | 28/06/2013 | HR Director | Mr. R.Kumar | ISH |
| 1.7 | 21/06/2014 | HR Director | Mr. R.Kumar | ISH |
| 1.8 | 01/08/2014 | HR Director | Mr. R.Kumar | ISH |
| 1.9 | 22/06/2015 | HR Director | Mr. R.Kumar | ISH |
| 2.0 | 14/06/2016 | HR Director | Mr. R. Kumar | ISH |
| 2.1 | 15/11/2017 | HR Director | Mr. R. Kumar | ISH |
| 2.2 | 12/06/2018 | HR Director | Mr. R. Kumar | ISH |
| 2.3 | 10/07/2019 | HR Director | Mr. R. Kumar | ISH |
| 2.4 | 09/11/2020 | HR Director | Mr. R. Kumar | ISH |
| 2.5 | 06/12/2021 | HR Director | Mr. R. Kumar | ISH |
| 2.6 | 02/12/2022 | HR Director | Mr. R. Kumar | ISH |

## 1. PURPOSE

This policy provides a set of requirements for the regulation of special access use on the AEL Data Systems and Network.

## 2. SCOPE

This policy will provide a mechanism for the addition and removal of people from the special access status and a mechanism for periodic reviews of the special access status.

## 3. RESPONSIBILITIES

The responsibility of effective implementation of this policy lies with IT & IS Head.

## 4. REFERENCE STATEMENTS

### 4.1. Regulation of special access accounts

4.1.1. Special access on AEL Data systems is maintained and monitored at the discretion of AEL Data.
4.1.2. Individuals authorized to receive special access elevation or passwords must sign a form which is available with CISO.
4.1.3. Special access is only provided to individuals who need said access to perform their job.
4.1.4. Any misuse of special access privileges must be reported immediately to the CISO

### 4.2. Acquiring special access

4.2.1. It is strongly suggested all persons requesting special access complete a Special Access Request form. A separate form should be completed for each Special Access Requirement. The same should be approved by process owner.

4.2.2. All persons requesting special access must read and sign the Special Access Guidelines Agreement. This agreement discusses the do's and don'ts of using special access. Once a person signs the agreement he/she is then bound to abide by its contents. The signed originals should be kept with IT Services Operations Manager.

4.2.3. Any person refusing to sign the Special Access Guidelines Agreement will not be provided special access.

4.2.4. In case of change in special access requirements, the covered persons must inform the CISO about the change immediately.

### 4.3. Performing a periodic review of the special access

4.3.1. A review of special access status will be made on a quarterly basis or as determined by the CISO or the appropriate resource administrator.

4.3.2. Two reports have significance. One report lists special access by system and access type. The second report lists the access by person (i.e., for each person, all access given to that person is listed).

4.3.3. If anyone determines that an individual needs to be added to other special access groups, that individual must submit a Special Access Request form requesting additional access to the appropriate resource administrator (e.g., print operators, power users)

### 4.4. Removing people from the special access status

4.4.1. A person may be removed from the special access status for one of three reasons:

- The person no longer works at AEL Data
- The person no longer needs special access due to a change in job duties
- The person has violated the Special Access Guidelines Agreement.

4.4.2. A person may be removed from the special access status at any time as determined by AEL Data CISO or resource administrator immediately with sign a off.

## 5. COMPLIANCE

5.1. Audits will be performed on a regular basis by authorized organizations/designated officers of AEL Data.

5.2. Audits will be managed in accordance with the Information Security Audit Procedure.

5.3. Every effort will be made to prevent audits from causing operational failures or disruptions.

## 6. EXCLUSIONS

There are no exclusions to the above guidelines

## 7. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action as per HR & Admin Procedure.