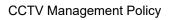


CCTV Management Policy

CCTV Management Policy

Version 2.8

Document version control page



|--|

Prepared By

	A 4 h. a	Undate Description	
Date	Author	Update Description	
12/06/08	JayaseelanJ	Initial Issue	
22/08/08	JayaseelanJ	Format changes	
10/09/09	JayaseelanJ	Policy Document Reviewed	
12/07/2010	J.Jayaseelan	Policy Document Reviewed	
25/11/2011	Jayaseelan J	Policy Document Reviewed and ISM Name changed to ISH	
27/06/2012	Jayaseelan J	Policy Document Reviewed	
27/06/2013	Jayaseelan J	 Policy Document Reviewed Point 4.4 " All the surveillance cameras are identified by the singe "CCTV Camera" is removed from the class 4. Reference Statement Point 4.2 and 4.3 updated 	
27/06/2013	Jayaseelan J	Policy Document Reviewed	
01/08/2014	Jayaseelan J	Policy Document Reviewed as per ISO 27001:2013 requirement	
22/06/2015	Jayaseelan J	Policy Document Reviewed	
14/06/2016	Jayaseelan J	Policy Document Reviewed	
15/11/2017	Santhosh S	Policy Document Reviewed	
12/06/2018	Santhosh S	Policy Document Reviewed	
10/07/2019	Santhosh S	Policy Document Reviewed	
09/11/2020	Santhosh S	Policy Document Reviewed	
06/12/2021	Santhosh S	Policy Document Reviewed	
02/12/2022	Santhosh S	Policy Document Reviewed	
05/12/2023	Muthukrishnan B	Policy Document Reviewed	
04/12/2024	Muthukrishnan B	Policy Document Reviewed	
	10/09/09 12/07/2010 25/11/2011 27/06/2012 27/06/2013 27/06/2013 01/08/2014 22/06/2015 14/06/2016 15/11/2017 12/06/2018 10/07/2019 09/11/2020 06/12/2021 02/12/2022 05/12/2023	22/08/08 JayaseelanJ 10/09/09 JayaseelanJ 12/07/2010 J.Jayaseelan 25/11/2011 Jayaseelan J 27/06/2012 Jayaseelan J 27/06/2013 Jayaseelan J 27/06/2013 Jayaseelan J 27/06/2013 Jayaseelan J 27/06/2013 Jayaseelan J 21/06/2014 Jayaseelan J 22/06/2015 Jayaseelan J 22/06/2015 Jayaseelan J 14/06/2016 Jayaseelan J 15/11/2017 Santhosh S 12/06/2018 Santhosh S 10/07/2019 Santhosh S 09/11/2020 Santhosh S 02/12/2021 Santhosh S 02/12/2021 Santhosh S 02/12/2021 Santhosh S 02/12/2023 Muthukrishnan B	

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

	- <u>-</u>	0	CCT\	/ Management Policy
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
2.7	05/12/2023	HR Director	Mr. R. Kumar	ISH
2.8	04/12/2024	HR Direvtor	Mr.R.Kumar	ISH



1. PURPOSE

CCTV Management Policy is to establish a framework to monitor the data centre by the adopted Camera devices within AEL Data. AEL Data adoption of recommended standards and associated conformity assessment programs will help the Organisation to enhance the security at data centre by effective use of Surveillance camera device.

2. SCOPE

This policy applies to the entire Departments of AEL Data to ensure the effective use of Surveillance camera.

3. ROLES AND RESPONSIBILITIES

The responsibility of effective implementation of this policy lies with Information Security Head and IT Dept.

4. REFERENCE STATEMENTS

- 4.1. CCTV will be monitored by IT/IS Dept and Security Guard all the time.
- 4.2. The Surveillance camera outputs are recorded as movie documented information's in the DVR system.
- 4.3. The back-up of the movie documented information's are stored in the DVR System are backuped in DVD & Tapes.

1. COMPLIANCE

- 1.1. Audits will be performed on a regular basis by authorized organizations/designated officers of AEL Data.
- 1.2. Audits will be managed in accordance with the Information Security Audit Procedure.
- 1.3. Every effort will be made to prevent audits from causing operational failures or disruptions.

2. EXCLUSION

There are no exclusions to the above guidelines

3. ENFORCEMENT

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