PLANETCAST MEDIA SERVICES LIMITED

ISMS Policy

Document Release History

Version	Review Date	Approval Date	Preparation Date	Prepared By	Updated/Reviewed by	Approved by
1.0	16th Feb 2009	16th Feb 2009	15th Feb 2009	Manish Badoni	Nutesh	N.K.Badola
1.0	4th Jan 2010	6th Jan 2010	-	-	Nutesh	N.K.Badola
2.0	28th Dec 2011	2nd Jan 2012	-	Rachna Tripathi	Sanjeev Bajaj	Rajesh Yadvendu
2.0	2nd Jan 2013	2nd Jan 2013	-	Sanjeev Bajaj	Rajesh Yadvendu	Rajesh Yadvendu
2.0	22nd March 2013	22nd March 2013	-	-	Rajesh Yadvendu	Rajesh Yadvendu
3.0	12th Jan 2014	13th Jan 2014	-	-	Rajesh Yadvendu	Rajesh Yadvendu
3.0	8th Jan 2015	9th Jan 2015	-	-	Rajesh Yadvendu	Rajesh Yadvendu
3.1	8th Jan 2016	9th Jan 2016	-	-	Rajesh Yadvendu	Rajesh Yadvendu
3.1	8th March 2016	9th March 2016	-	-	Rajesh Yadvendu	Sanjay Duda
3.1	9th March 2017	9th March 2017	-	-	Rajesh Yadvendu	Sanjay Duda
3.1	14th February 2018	14th February 2018	-	-	Rajesh Yadvendu	Sanjay Duda
3.1	8th February 2019	11th February 2019	-	-	Rajesh Yadvendu	Sanjay Duda

Document Maintenance

Version	Description of Change	Chapter/ Section/ Page	Date	Updated/Reviewed by
2.0	First page Document control format changed.	Page 1	28th Dec 2011	Sanjeev Bajaj
2.0	Enforcement of area added here.	Page 5	28th Dec 2011	Sanjeev Bajaj
2.0	Point of contact was changed	Page 5	28th Dec 2011	Sanjeev Bajaj
3.0	Objective was modified	Page 2	12th Jan 2014	Sanjeev Bajaj
3.1	Reissue due to org. changed	-	9th March 2016	Sanjeev Bajaj

Prepared by	Reviewed by	Approved by
Sanjeev Bajaj	Rajesh Yadvendu	Sanjay Duda

Document Custodian

Version	Document Type (Printed/ Electronic)	Custodian of Document
3.1	Electronic	ISO

Document Distribution

Name	Title	Department	Version	Document Type (Printed/ Electronic)	Approval Date
Sanjeev Bajaj	Jt..G.M	HUB	3.1	Electronic	11th February 2019

PMSL'S ISMS POLICY

1-Objective

PMSL's objective of managing information security is to ensure that it's Hub/ISP and all other Playout operation and supporting business operations continue to operate with minimal disruptions.

PMSL shall ensure that all information that are disbursed or produced by PMSL have absolute integrity.

PMSL shall guarantee that all information are managed and stored with appropriate confidentiality procedures.

2-POLICY

The purpose of the policy is to protect the organization's information assets from all threats, whether internal or external, deliberate or accidental.

It is the policy of the organization to ensure that:

- Information should be made available with minimal disruption to staff and the public as required by the business process;
- The integrity of this information will be maintained;
- Confidentiality of information not limited to research, third parties, personal and electronic communication data will be assured;
- Regulatory and legislative requirement will be met;
- A Business Continuity Management Framework shall be available and business continuity plan will be produced to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. Business continuity plans should be maintained and tested.
- Information security education, awareness and training will be made available to staff.
- All breaches of information security, actual or suspected, will be reported to, and investigated by the CISO and his designated team.
- Appropriate access control will be maintained and information is protected against unauthorized access.
- Policies procedures and guidelines not limited to information security will be made available in both hard copy and online format through an internet system to support the ISMS policy.
- ISMS team has been directed responsibility for maintaining the ISMS Policy and involved with writing and/or managing the development of relevant policies, procedures and guidelines not limited to information security.
- All Managers are directly responsible for implementing the ISMS Policy within their units, and for

adherence by their staff.

- It is the responsibility of each member of staff to adhere to the ISMS Policy.
- Information security is managed through PMSL's Risk Management Framework.
- The availability of information and information system will be met as required by the core and supporting business operations.
- Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, Sent by fax, stored on tapes and diskettes, or spoken in conversation and over the telephone.
- This will ensure that information and vital services are available to users when and where they need them.
- Safeguarding the accuracy and completeness of information by protecting against unauthorized modification.
- The protection of valuable or sensitive information from unauthorized disclosure or unavoidable interruption.
- This will ensure that the organization remains complaint to relevant business, national and international laws and it includes meeting the requirements stated in legislation such as the IT act 2000, Companies Act and the data protection Act.
- Business continuity Management should be implemented effectively to ensure continuity of business operations in the event of a crisis or disaster.
- Ensure that relevant and effective training are provided to staffs.
- Ensure that the staff understand their roles and responsibility in handling incidents and have a comprehensive and well tested incident response plan ready.

The policy will be reviewed and updated (if required) by PMSL ISMS Team annually.

3-Point of Contact

For clarification or further information on this policy, contact Chief Information Security Officer.

4-Enforcement

- All users shall read and abide by this ISMS Policy.
- Any employee found in violation to this policy shall be subjected to disciplinary action as mentioned under PMSL-ISMS-PO-020-Employee Discipline Policy.

Executive Director **Dated:** 11th February 2019