PLANETCAST MEDIA SERVICES LIMITED
Information Security 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	Rajesh Yadvendu
1.0	4th Jan 2010	6th Jan 2010	-	-	Nutesh	Rajesh Yadvendu
2.0	28th Dec 2011	2nd Jan 2012	-	-	Sanjeev Bajaj	Rajesh Yadvendu
2.0	2nd Jan 2013	2nd Jan 2013	-	-	Sanjeev Bajaj	Rajesh Yadvendu
2.0	22nd March 2013	22nd March 2013	-	-	Sanjeev Bajaj	Rajesh Yadvendu
3.0	18th April 2014	19th April 2014	-	-	Sanjeev Bajaj	Rajesh Yadvendu
3.0	18th April 2015	19th April 2015	-	-	Sanjeev Bajaj	Rajesh Yadvendu
3.0	18th April 2015	19th April 2015	-	-	Sanjeev Bajaj	Rajesh Yadvendu
3.1	7th March 2016	7th March 2016	-	-	Sanjeev Bajaj	Sanjay Duda
3.1	7th March 2017	7th March 2017	-	-	Sanjeev Bajaj	Sanjay Duda
3.1	13th February 2018	13th February 2018	-	-	Sanjeev Bajaj	Sanjay Duda
3.1	8th February 2019	11th February 2019	-	-	Sanjeev Bajaj	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	28thDec 2011	Sanjeev Bajaj
2.0	Review of Policy frequency was defined.	Page 2	28thDec 2011	Sanjeev Bajaj
3.0	Some point added in policy	Page 2	18th April 2014	Sanjeev Bajaj
3.1	Reissued due to Organisation re-branding.	---	7th March 2016	Sanjeev Bajaj

Document Custodian

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

Prepared By	Reviewed By	Approved By
Manish Badoni	Sanjeev Bajaj	Sanjay Duda

Document Distribution

Name	Title	Department	Version	Document Type (Printed/ Electronic)	Approval Date
Sanjay Duda	CISO	Technical	3.1	Electronic	11th February 2019

Prepared By	Reviewed By	Approved By
Manish Badoni	Sanjeev Bajaj	Sanjay Duda

PMSL's Information Security Policy

1.Objective: PMSL objective for Information Security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents and where possible, prevent their occurrence.

2. Purpose: To protect the organization's information assets from all threats and vulnerabilities, whether internal or external, deliberate or accidental. At all times, the cost effectiveness and fitness for purpose of countermeasures will be considered.

3. Policy: It is the Policy of the Organization to ensure that:

- It is appropriate to the purpose of the organization.
- It includes a framework for setting information security objectives, including structure of risk assessment and risk treatment.
- The information security objectives shall be consistent with information security policy & be measurable, communicative and updated as appropriate.
- It includes a commitment to satisfy applicable requirements related to information security.
- It includes a commitment to continual improvement of the information security management system.
- Critical information is protected from unauthorized access, use, disclosure, modification and disposal, whether intentional or unintentional.
- The confidentiality, integrity and availability of such information acquired permanently or in transit, provided or created are ensured at all times.
- All breaches of information security, actual or suspected, are reported, investigated by the designated personnel and appropriate corrective and preventive actions initiated.
- Awareness programs on Information Security are available to all employees and wherever applicable to third parties e.g. Sub-contractors, consultants, vendors etc. and regular training is imparted to them.
- A Business Continuity Plan is maintained and tested.
- All legal and contractual requirements with regard to information security are met wherever applicable.
- The policy will be reviewed at periodic intervals either annually or as appropriate to check for its effectiveness, changes in technology, and changes in risk Levels that may have impact on Confidentiality, Integrity and Availability, legal and contractual requirements, and business efficiency. Procedures exist to support the policy.
- It is the responsibility of all employees to understand and adhere the Information Security Policy. The Management reserves all rights to take disciplinary action in case of its violation.

4. Point of Contact:

For Clarification or further information on this policy, Contact Chief Information Security Officer.

5. Enforcement:
- All Users shall read and abide by this Information Security 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.

Chief Information Security Officer: **Dated: 11th February 2019**

Prepared By	Reviewed By	Approved By
Manish Badoni	Sanjeev Bajaj	Sanjay Duda