



PLANETCAST MEDIA SERVICES LIMITED

ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 1 of 27	Ver. No. 9.0

PLANETCAST MEDIA SERVICES LIMITED

ISMS Manual

Document Release History

Version	Review Date	Approval Date	Preparation Date	Prepared By	Reviewed By	Approved By
1.0	15 th Feb 2009	16 th Feb 2009	15 th Feb 2009	Nutesh	Sanjeev Bajaj	N.K. Badola
1.0	4 th Jan 2010	6 th Jan 2010	-	-	Sanjeev Bajaj	N.K. Badola
2.0	28 th Dec 2011	2 nd Jan 2012	-	Rachna Tripathi	Sanjeev Bajaj	Rajesh Yadvenu
2.0	14 th April 2012	14 th April 2012	-	-	Sanjeev Bajaj	Rajesh Yadvenu
3.0	1 st Feb 2013	1 st Feb 2013	-	-	Sanjeev Bajaj	Rajesh Yadvenu
4.0	13 th Jan 2014	13 th Jan 2014	-	-	Sanjeev Bajaj	Rajesh Yadvenu
4.0	18 th April 2014	19 th April 2014	-	-	Sanjeev Bajaj	Rajesh Yadvenu
4.1	15 th March 2015	16 th March 2015	-	-	Sanjeev Bajaj	Rajesh Yadvenu
4.2	7 th Jan 2016	7 th Jan 2016	-	-	Sanjeev Bajaj	Rajesh Yadvenu
5.0	9 th March 2017	10 th March 2017	-	-	Sanjeev Bajaj	Sanjay Duda
6.0	14 th Feb 2018	15 th Feb 2018	-	Vishal Kaushik	Sanjeev Bajaj	Sanjay Duda
7.0	8 th Feb 2019	11 th Feb 2019	-	Mayank Kashkari	Sanjeev Bajaj	Sanjay Duda
8.0	3 rd February 2020	3 rd February 2020	-	Kartikey Datta	Sanjeev Bajaj	Sanjay Duda
8.0	3 rd Feb 2021	3 rd Feb 2021	-	-	Sanjeev Bajaj	Sanjay Duda
8.0	3 rd Feb 2022	3 rd Feb 2022	-	-	Sanjeev Bajaj	Sanjay Duda
9.0	4 th Feb 2022	4 th Feb 2022	-	-	Sanjeev Bajaj	Sanjay Duda

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda




PLANETCAST MEDIA SERVICES LIMITED

ISMS Manual	Preparation Date 15 th Feb 2009
	Review Date 3 rd February 2022
Doc. Classification: Internal	Approval Date 3 rd February 2022
Doc. No.: PMSL-ISMS-MD-001	Page 2 of 27 Ver. No. 9.0

Document Maintenance

Version	Description of Change	Chapter / Section / Page	Date	Updated / Revised By
2.0	First page Document control format changed.	Page 1	28th Dec 2011	Sanjeev Bajaj
2.0	PMSL vision and mission added.	Page 3,4	28th Dec 2011	Sanjeev Bajaj
2.0	ISMS Team added.	Page 7	28th Dec 2011	Sanjeev Bajaj
2.0	ISMS Team roles and responsibilities added.	Page 8	28 th Dec 2011	Sanjeev Bajaj
2.0	References of all documents at various places in the document were changed.	---	28 th Dec 2011	Sanjeev Bajaj
2.0	List of all documents added under appendix A.	Page 17	28 th Dec 2011	Sanjeev Bajaj
3.0	Three documents added. Refer to serial No-34,35,7	Page 7	1 st Feb 2013	Sanjeev Bajaj
4.0	Context of organization added	Page -6	13 th Jan 2014	Sanjeev Bajaj
4.0	Updation in all Sections	--	13 th Jan 2014	Sanjeev Bajaj
4.1	Some forms are deleted in Appendix-A	Page-27	16 th March 2015	Sanjeev Bajaj
5.0	ISMS Org chart updated	Page-10	9 th March 2017	Sanjeev Bajaj
6.0	ISMS Org chart updated (CI 7) Information Security Team Table Updated (CI 8)	Page-8	15 th Feb 2018	Sanjeev Bajaj
7.0	ISMS Org chart updated (CI 7)	Page-8	11 th Feb 2019	Sanjeev Bajaj
7.0	Addition of new policy of "Data Leakage Prevention Policy."	Page-22	11 th Feb 2019	Sanjeev Bajaj
8.0	ISMS Org chart updated (CI 7)	Page-8	3 rd February 2020	Sanjeev Bajaj
8.0	Scope of Statement Updated – SOA Revision Date Organization Chart Updated	Page-7 Page-9	3 rd February 2020	Sanjeev Bajaj
8.0	Scope of Statement Updated – SOA Revision Date Organization Chart Updated	Page-7 Page-9	3 rd February 2021	Sanjeev Bajaj
9.0	Scope of statement update-SOA updated, Organization Chart updated	Page-7, Page-9		

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 3 of 27	Ver. No. 9.0

Document Maintenance

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

Document Distribution

Name	Title	Department	Version	Document Type	Approval Date
Sanjay Duda	CISO	ISMS Team	8.0	Electronic	4 th February 2022

Contents

1. Introduction	5
2. PMSL Objective	6
3. Context of Organization	6
4. Interested Parties	7
5. ISMS Scope	7
6. Information Security Management System	8
7. Organization of Information Security (Internal Organization- ISMS Team)	9
8. Information Security Team - Roles, responsibilities and authorities	9
9. Leadership and Commitment:	10
10. Information Security Policy	11
11. Risk Assessment Approach	11
12. Risk Treatment	12
13. Information Security Objectives and Planning	13
14. Statement of Applicability	13
15. ISMS Implementation and Operation	13

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda



PLANETCAST MEDIA SERVICES LIMITED

ISMS Manual

Preparation Date 15th Feb 2009

Review Date 3rd February 2022

Doc. Classification: Internal

Approval Date 3rd February 2022


Doc. No.: PMSL-ISMS-MD-001

Page 4 of 27

Ver. No. 9.0

16. Monitor and Review the ISMS	14
17. ISMS Maintenance and Improvement	15
18. Resource Management	15
18.1 Resource Provision	15
18.2 Training Awareness and Competency	15
18.3 Communication	16
19. Documentation Requirements	16
20. General.....	16
21. Control of Documented Information	17
22. Internal ISMS Audit	17
23. Management Review of the ISMS	18
24. ISMS Improvement	18
a. Corrective Actions	18
b. Continual Improvement	19

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 5 of 27	Ver. No. 9.0

1. Introduction

Planetcast Media Services Limited is a key market player in providing technology-led managed services to the broadcasting industry in India & neighboring countries with rapidly growing footprint across Southeast Asia.


We provide comprehensive, customized solutions across content management operations (including content storage, enrichment and automated play-out) and distribution (including satellite broadcasting/ up-linking, digital streaming and cloud distribution). We are proud that we are held in high esteem in the outsourced distribution and play-out services segment in India.

We provide end-to-end solutions across key segments of the broadcast content delivery chain. With a robust track record of nearly two successful decades, we have been offering most agile and state-of-the-art services to broadcasters. We are driven by a passion to help business units build stronger and innovative services.

PLANETCAST enables global enterprises make their operations as efficient and cost-effective as possible, thereby unleashing new potential across organizations. Our uniqueness lies in our ability to assist customers meet complex technical and operational challenges, and thereby enhance productivity.

PLANETCAST ability to conceptualize, architect and implement new and expanded capabilities allows client stake their business to then next level.

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 6 of 27	Ver. No. 9.0

2. PMSL Objective

- One of the largest technology-led managed service provider for the Indian Broadcasting Industry.
- Sustained value-add to customers in content delivery services.
- We truly understand that content operations and distribution services are mission critical for broadcasters.
- We provide tailored solutions for customers specialized business needs.
- Our uniqueness lies in end-to-end services across the content delivery chain ,catering to multiple formats channels and delivery mechanisms.
- Cutting edge technology adapted to Indian market requirements, ensure ensures reasonable pricing and flexible solutions
- We ensure your business never skips a beat, even in the face of disaster.
- PLANETCAST–A true24x7x365Company

3. Context of Organization

PMSL determines complete internal and external issues that are relevant to its business operations and that affect its ability to achieve the intended outcomes of ISMS. Refer to clause-4.1

Those can be categories into two subcategories:

- ✓ External Issues
- ✓ Internal Issues

External Issues	Internal Issues
Stakeholder expectation	Organization culture
Competitors business strategy	Objective, strategies and policies
Local Effects of Natural disaster	Change Management Procedure
Contractual requirements of Third parties, vendors, service providers	Availability of Knowledge, skill and resources
Organisation Legal Obligations	Local Environmental controls
Clients Agreement & Contractual Obligations	Financial, physical and intellectual assets.
Customer Satisfaction	Business and service continuity capabilities
Market Trends	Compliance approach with legal and contractual obligations
Government regulations	Our vision and values
Technological Advancement & Changes	Contractual relationship
Impact of Cultural, Social, Political trends	Brand reputation

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda



ISMS Manual

Preparation Date 15th Feb 2009

Review Date 3rd February 2022

Doc. Classification: Internal

Approval Date 3rd February 2022

Doc. No.: PMSL-ISMS-MD-001

Page 7 of 27

Ver. No. 9.0

	Employees Motivation
	Profitability Situation
	Information system and processes
	Standard, guidelines and models adopted by the organization

4. Interested Parties

PMSL determines interested parties, and the requirement of these interested parties:


External Interested Parties	Requirements
Stakeholder (Internal Departments)	Managed IT operations
Emergency Services (Eg. Fire fighters, police, ambulance etc)	Timely and correct information about eventuality
Service Providers for leased lines, ISP etc.	Clearly defined service level requirements
Customer providing Media	CIA of the Media and timely operation
User / Consumer of product/services Market in which PMSL operates	Genuine products
Customers, suppliers, vendors	Clearly defined Supply requirements
Government regulation	Compliance to applicable regulations

Internal Interested Parties	Requirements
Board of Directors	Compliance to corporate policies.
Company Secretary / Compliance Team of the Firm	Tracking of compliance to applicable requirements
Partners	Clearly defined MOU
Executive Committee	Clearly defined jurisdiction and responsibilities
Employees	Clearly defined directions and compensation
Third Party Resources	Clearly defined Charter of Duties and SLA

5. ISMS Scope

“The management of information security as it applies to Network Operations Center services which Comprises of Hub & ISP and Playout facilities including STAR, Disney, Viacom and NGC from its location at Noida & Mumbai supported by IT, HR, Administration, Maintenance and Legal Departments. This is in accordance with statement of applicability Ver. 6.1 Dated 4th February 2022”

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 8 of 27	Ver. No. 9.0

For details, Refer PMSL-ISMS-MD-002 Scope Statement

6. Information Security Management System

The management of PMSL is committed to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS. It has directed the task of risk assessment and treatment guidelines and monitors the ISMS by means of regular reviews. It has ensured this by establishing an information security policy that lays down the information security objectives and plans as well as establishing roles and responsibilities for information security. It also provides sufficient resources to develop, implement, operate and maintain the ISMS.

PMSL depends upon the correct and efficient working of its Information Technology (IT) infrastructure. Problems affecting the IT infrastructure could cause tangible or intangible damage to PMSL or even its stakeholders.


PMSL establishes its information security management system based on ISO 27001 Standard, as this fulfills PMSL's Information Security needs.

The use of ISO 27001 controls, and other best practices identified by PMSL's own team will help PMSL to achieve its security needs.

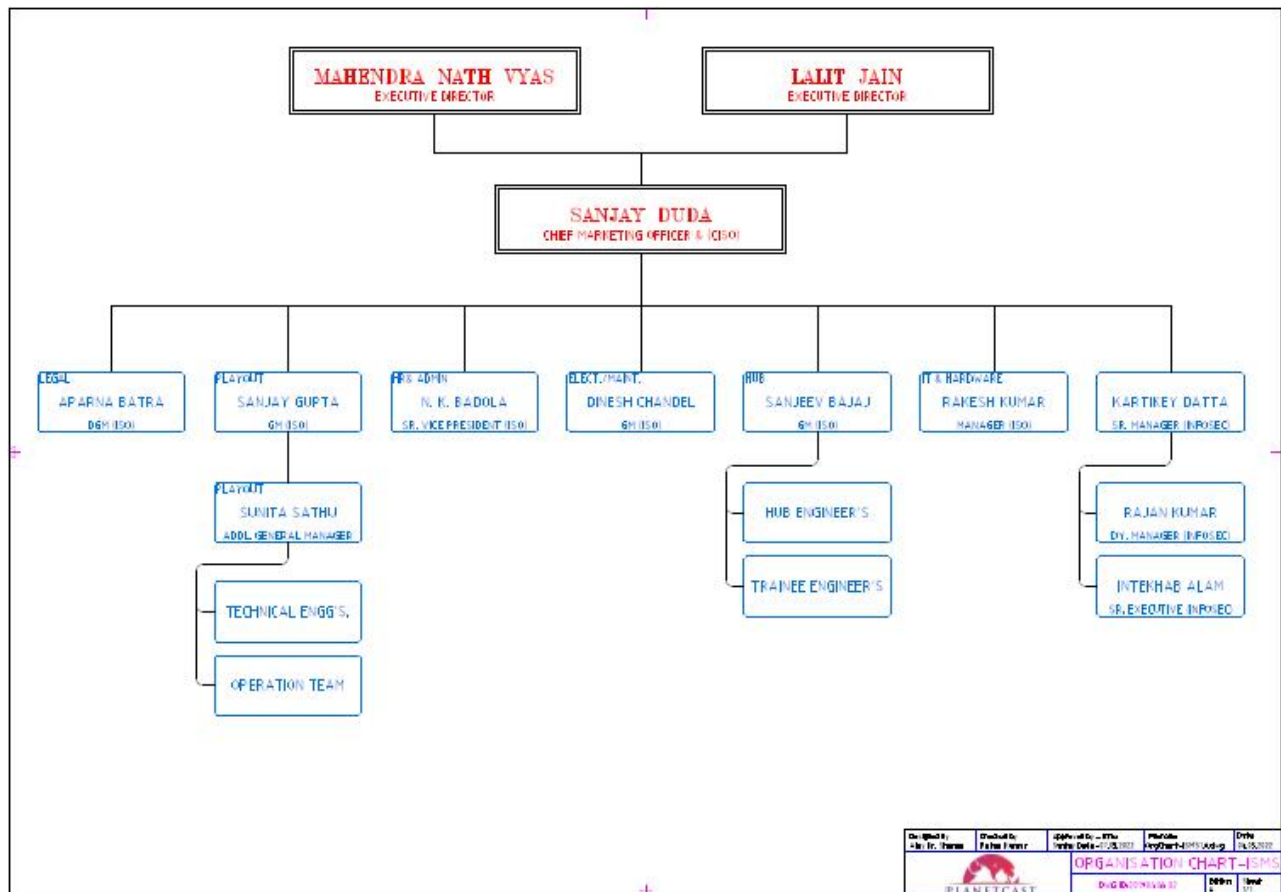
Information security management system identifies the adequate level of protection for all information assets with regard to a number of information security principles, such as confidentiality, Availability, and Integrity, and ensures that all assets are protected accordingly. To reach this goal, it has to provide efficient technical and organizational security measures such as Risk Assessment and Risk Management, which are recurring information Security Processes for PMSL.

PMSL achieves continual improvement of its Information Security Management System.

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 9 of 27	Ver. No. 9.0


7. **Organization of Information Security (Internal Organization- ISMS Team)**



8. **Information Security Team - Roles, responsibilities and authorities**

Top management shall ensure that the responsibilities and authorities for roles relevant to

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 10 of 27	Ver. No. 9.0

information security are assigned and communicated, in addition to ensure the Compliance of ISO 27001 in all the supporting departments of PMSL. PMSL has identified the list of ISMS Team SPOC:-

Department Name	ISMS Team SPOC (ISOs)
IT	Rakesh Kumar
Admin	Sanjeev Kumar Malik
HR	Shweta Ranjan
E & M	Dinesh Chandel
Legal	Aparna Batra
HUB	Sanjeev Bajaj
Star & Other Payout	Sunita Sathu

- Responsibilities of ISMS Team SPOCs
- To implement & Operate ISMS in their own department.


Roles & Responsibilities of Information Security Team.(Ref:PMSL-ISMS-PR-011-Information Security Responsibilities Procedure).

9. Leadership and Commitment:

PMSL's Top management demonstrate leadership and commitment with respect to ISMS by:

1. Ensuring that Information Security Policy and Information Security objectives are established and are also compatible with strategic direction of PMSL;
2. Ensuring the integration of the Information security management system requirements in to the PMSL processes;
3. Ensuring that resources needed for Information Security management system are available.
4. Communicating the importance of effective information security management and of conforming to the information security management system requirements;
5. Ensuring that the information security management system achieves its intended outcome(s);
6. Promoting Continual Improvement;

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 11 of 27	Ver. No. 9.0

7. Supporting other relevant management roles to demonstrate their leadership as it applies to their area of responsibility.

10. Information Security Policy

PMSL’s Top management shall establish an information security Policy that-

- 1-It is appropriate to the purpose of the Organization;
- 2-It includes information security objectives or provides the framework for setting information security objectives;
- 3-Communications to all concerned persons within the organization, stressing the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement are regularly sent;

Information Security has been established in a way that it is well communicated within organization and be available to interested parties.


Information Security Policy is covered in “Information Security Policy”. For details, Refer PMSL-ISMS-PO-028-Information security Policy

11. Risk Assessment Approach

PMSL shall define and apply an information security risk assessment process that:-

- a) establishes and maintains information security risk criteria that include:
 - 1) the risk acceptance criteria;
 - 2) Criteria for performing information security risk assessments;
- b) ensure that repeated information security assessments produce consistent, valid and comparable results;
- c) Identifies the information security risks:
 - 1) apply the information security risk assessment process to identify risks associated with loss of confidentiality, Integrity and availability for information with in scope of the ISMS.
 - 2) Identify the risk owner

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 12 of 27	Ver. No. 9.0

d) analysis the information security risk :

- 1) assess the potential consequences that would result if the risks identified in 11.c)1) were to materialize,
- 2) Assess the realistic likelihood of the occurrence of the risks identifies in 11.c)
- 3) Determine the level of risk,

e) evaluates the information security risks :

- 1) compare the result of risk analysis with the risk criteria established in 11.a) and
- 2) Prioritize the analyzed risks for risk treatment.

12. Risk Treatment

Based on the Risk Assessment, PMSL has established a program for reducing risk for any assets where the risk is beyond the acceptable limits. For each of the risks identified following the risk assessment a risk treatment decision needs to be made.


Possible options for risk treatment include:

- a) Selecting appropriate information security risk treatment options,
- b) Applying appropriate controls to reduce the risks;
- c) Comparing the applied controls and check that no control has been omitted.
- d) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance;
- e) avoiding risks by not allowing actions that would cause the risks to occur;
- f) Transferring the associated risks to other parties, e.g. insurers or suppliers.

For those risks where the risk treatment decision has been taken, apply appropriate controls, these controls should be selected and implemented to meet the requirements identified by a risk assessment.

Controls should ensure that risks are reduced to an acceptable level taking into account:

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 13 of 27	Ver. No. 9.0

- a) requirements and constraints of national and international legislation and regulations;
- b) organizational objectives;
- c) operational requirements and constraints;
- d) cost of implementation and operation in relation to the risks being reduced, and remaining proportional to the organization’s requirements and constraints;
- e) the need to balance the investment in implementation and operation of controls against the harm likely to result from security failures.

It is kept in mind that no set of controls can achieve complete security, and that additional management action may need to be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls to support the organization’s aims.

- g) Obtain risk owners approval of the information security risk treatment plan and acceptance of the residual information security risks.

13. Information Security Objectives and Planning

PMSL shall establish information security objectives at relevant functions and levels. For details, refer PMSL-ISMS-PO-035-ISMS Objectives.

14. Statement of Applicability


Pursuant to the requirements of the ISO 27001 standard, PMSL has identified the controls, which are deemed by it to be applicable for managing the risk of those entities covered within the ISMS. The controls are selected from the options included in Annex A of the ISO 27001 standard.

Statement of Applicability is covered in “Statement of Applicability” document.

For details, Refer PMSL-ISMS-MD-006-Statement of Applicability

15. ISMS Implementation and Operation

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 14 of 27	Ver. No. 9.0

ISMS team of PMSL will carry out the following information security related tasks.

- Plan and implement the risk treatment measures determined as per the risk treatment plan described above. (The plan identifies the appropriate management action, responsibilities and priorities for managing information security risk.)
- Implement training and awareness programs for general users.
- Manage the resources and operations for effective information security.
- Assist in identifying and implementing procedures and other controls capable of enabling prompt detection of and response to security incidents.

16. Monitor and Review the ISMS


The ISMS is monitored and reviewed periodically (i.e. annually or as & when required) to improve its functioning in the following areas.

- Detection of security risks that may impact effective functioning of PMSL
- Identification of failed and successful security breaches and its response capability in this area.
- Enable the management to determine whether the security activities delegated to people or implemented by information technology are being performed as expected;
- Swift and effective action taken to resolve a breach of security reflecting business priorities.

Effectiveness of the ISMS will be reviewed (Including meeting security policy and objectives, and review of security controls) by Information Security Team, taking into account result of security audits, incidents, suggestions and feedback from all interested parties. Reviews take into account the following aspects while evaluating effectiveness and recommending further action.

- Organization
- Technology
- Business objectives and processes
- Identified risks
- Changes in external operating environment that may affect functioning

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 15 of 27	Ver. No. 9.0

17. ISMS Maintenance and Improvement

PMSL uses the data from the Security Reviews to take action for improvement in the following areas.

- Implement the identified improvements in the ISMS, including corrective actions, in a manner as identified by the management.
- Apply the lessons learn from the security incidences.
- Communicate the results of the ISMS review and expected action to all relevant parties and try to arrive at a common plan.
- Check that the improvements achieve their intended objective

18. Resource Management

18.1 Resource Provision


PMSL has determined the requirements and provided necessary resources needed to establish, implement, operate and maintain the ISMS. This is in order to ensure that information security procedures support the business requirements, identify and address legal and regulatory requirements and contractual security obligations, maintain adequate security by correct application of all implemented controls, carry out reviews when necessary, and to react appropriately to the result of these reviews including improvements of the ISMS.

18.2 Training Awareness and Competency

PMSL ensures that all personnel assigned responsibilities defined in the ISMS are competent to perform the required tasks. This is ensured by establishing several processes including the following:

- Providing competent training to deployed personnel.
- Maintaining records of education, training, skills, experience and qualifications of all personnel.
- Where applicable ,take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken,
- Persons should be aware of the Information security Policy,

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 16 of 27	Ver. No. 9.0

PMSL also ensures that all concerned personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives, by means of various user education activities.

18.3 Communication

PMSL has determine need for both internal and external communication

- Communication in PMSL is done whenever either the policy gets revised.
- It could be with suppliers, vendors, clients, customers, employees etc.
- It could be on IS policies, ISMS objectives, suppliers polices, or policies related to respective department. Refer to doc(PMSL-ISMS-PO-035 ISMS objective policy)
- Communication is done by CISO
- Communication of policies and other information in PMSL is done via:
 - Emails
 - Electronic board
 - Posters in case information is public, etc
 - Brochures
 - Letters
 - Face to Face Meetings etc.
- Refer to Doc : Communication Procedure [PMSL-ISMS-PR-025]

19. Documentation Requirements

20. General


The documentation maintained for the ISMS includes the following:

- Documented information required by international standard.
- Documented information determined by the Organisation.

All documentation is made available to users as required by the ISMS policy.

Documents and records may be in electronic or paper from. All effort will be made, within practicable limitations, to keep policy documents, records and control procedures in electronic form.

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 17 of 27	Ver. No. 9.0

21. Control of Documented Information

All ISMS documents are protected and controlled to ensure :

- Review and update documented information as necessary and re-approve amendment to the same.
- Ensure that changes and the current revision status of documented information are identified.
- Ensure that the most recent version of the relevant documented information is available at the points of use.
- Ensure that the documented information remain legible and identifiable.
- Ensure that documented information of external origin are identified.
- Ensure that the distributions of the documented information are controlled.
- Prevent unintended use of obsolete documented information .
- Apply suitable identification to the obsolete documents if they are retained for any purpose.

For details, Refer PMSL-ISMS-PR-001-Control of documented information

22. Internal ISMS Audit

Internal Audit team ensures that the PMSL, IT operations are conducted according to the highest standards by providing an independent, objective assurance function and by advising on best practice. Through a systematic and disciplined approach, Audit helps PMSL IT accomplish its objectives by evaluating and improving the effectiveness of risk management, controls and governance processes. As part of this process, Audit checks whether the ISMS conform to the requirements of ISO 27001 standard.

PMSL has:

- Planned, established and maintain an audit programme, the audit programme(s) shall take into the consideration the importance of the processes concerned and the results of previous audits,
- Define the audit criteria and scope for each audit,
- Selected the auditors and conducted the audit .
- Ensured results of audits are reported to relevant management.
- Retained documented information as evidence of audit programme.

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

The security risk assessments will be performed every year. Additional risk assessments may be conducted if so required by the business and operating environment and as deemed necessary by the Information Security Council.

The management responsible for the area being audited has to ensure that actions are taken without undue delay to eliminate deleted non-conformities and their causes.

Frequency as defined in the Internal Audit Procedure is Once in a year / annually or as an when required by the management whichever is earlier.

For details refer PMSL-ISMS-PR-003-Internal Audit Procedure

23. Management Review of the ISMS

The Information Security Team of PMSL reviews the organization’s ISMS at planned intervals (Annually or as & when required) to ensure its continuing suitability, adequacy and effectiveness. This includes assessing opportunities for improvement and requires changes to be clearly documented and records maintained as per defined procedure.

For details, refer: PMSL-ISMS-PR-002-Management review Meeting procedure


24. ISMS Improvement

PMSL shall take action to eliminate the cause of non-conformities with the ISMS requirements in order to prevent recurrence. The documented procedure for corrective action has defined requirements for:

a. Corrective Actions

- a) Identifying non-conformities;
- b) determining the causes of non-conformities;
- c) Determine if similar non conformities exist, or could potentially occur.
- c) determining and implementing the corrective action needed;

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 19 of 27	Ver. No. 9.0

- d) Evaluating the need for actions to ensure that non-conformities do not recur;
- e) recording results of action taken and
- f) review the effectiveness of any corrective action taken.
- g) Make changes to ISMS if necessary.

b. Continual Improvement

PMSL strives to continually improve the effectiveness of the ISMS through the use of the information security policy, audit results, analysis of monitored events and management review.

Details of ISMS Documents refer to Appendix -A below

Appendix – A

(I) LIST OF MANAGEMENT DOCUMENTS

S.No.	Document Description	Document Reference Number
1.	ISMS Manual	PMSL-ISMS-MD-001ISMS Manual
2.	Scope Statement	PMSL-ISMS-MD-002 Scope Statement
3.	Statement of Applicability	PMSL-ISMS-MD-006-Statement Of Applicability
4.	Master list of documents	PMSL-ISMS-MD-004 Master List of documents
5.	Master list of Records	PMSL-ISMS-MD-003- Master list of records
6.	Risk register (RA Sheet)	PMSL-ISMS-MD-005 Asset Register
7	RA Annexure B	PMSL-ISMS-MD-007-Annexure B - Risk Analysis & Assessment
8	Effectiveness of Controls	PMSL-ISMS-MD-008 Effectiveness of Controls
9	Effectiveness of Clauses	PMSL-ISMS-MD-009 Effectiveness of Clauses

(II) LIST OF ISMS MANDATORY DOCUMENTS

S.No.	Document Reference Number	Document Name	Clause No.
1	PMSL-ISMS-MD-002 Scope Statement	Scope of ISMS	4.3
2	PMSL-ISMS-PO-028-Information security Policy,PMSL-ISMS-PO-035-ISMS Objectives	Information security Policy & Objectives	5.2,6.2
3	PMSL-ISMS-PR-012-Risk Management Procedure	Risk assessment & Risk treatment methodology	6.1.2

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda



ISMS Manual

Preparation Date 15th Feb 2009

Review Date 3rd February 2022

Doc. Classification: Internal

Approval Date 3rd February 2022

Doc. No.: PMSL-ISMS-MD-001

Page 20 of 27

Ver. No. 9.0

4	PMSL-ISMS-MD-006-Statement Of Applicability	SOA	6.1.3 d
5	PMSL-ISMS-PL-003-Risk Treatment Plan	Risk Treatment Plan	6.1.3.e,6.2
6	PMSL-ISMS-PR-011 -Information Security Responsibilities Procedure	Security Roles & responsibility	A.7.1.2,A.13.2.4
7	PMSL-ISMS-PO-023- Acceptable Use Policy	Acceptable use of Policy	A.8.1.3
8	PMSL-ISMS-PO-004-Access Control Policy	Access Control Policy	A.9.1.1
9	PMSL-ISMS-SP-005-Standard Operating Procedure for IT	Operating procedure for IT	A.12.1.1
10	PMSL-ISMS-PO-33 -Secure System Engineering Principles Policy	Secure system engineering principles	A.14.2.5
11	PMSL-ISMS-PO-34 -Supplier Security Policy	Supplier Security Policy	A.15.1.1
12	PMSL-ISMS-PO-015-Incident Management Policy	Incident Management Policy	A.16.1.5
13	PMSL-ISMS-PR-024-BCP Procedure	Business Continuity Procedure	A.17.1.2

(III) LIST OF ISMS POLICIES

Sr. No.	Document Description	Document Reference Number
1.	Physical security Policy	PMSL-ISMS-PO-001-Physical security Policy
2.	Data Retention, Storage & Disposal of Media, Records Policy	PMSL-ISMS-PO-002-Data Retention, Storage & Disposal of Media, Records Policy
3.	Human resource security policy	PMSL-ISMS-PO-003-Human resource security policy
4.	Access Control Policy	PMSL-ISMS-PO-004-Access Control Policy
5.	Password policy	PMSL-ISMS-PO-005-Password policy
6.	Hardware & software management Policy	PMSL-ISMS-PO-006- Hardware & software management Policy
7.	Backup & Restore policy	PMSL-ISMS-PO-007- Backup & Restore policy

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda



PLANETCAST MEDIA SERVICES LIMITED

ISMS Manual

Preparation Date 15th Feb 2009

Review Date 3rd February 2022

Doc. Classification: Internal

Approval Date 3rd February 2022

Doc. No.: PMSL-ISMS-MD-001

Page 21 of 27

Ver. No. 9.0

8.	Network Devices Security Policy	PMSL-ISMS-PO-008- Network Devices Security Policy
9.	Remote Access Policy	PMSL-ISMS-PO-009- Remote Access Policy
10.	Router security policy	PMSL-ISMS-PO-010- Router security policy
11.	Personal Communication Devices Policy	PMSL-ISMS-PO-011- Personal Communication Devices Policy
12.	Email management Policy	PMSL-ISMS-PO-012- Email management Policy
13.	ISMS Policy	PMSL-ISMS-PO-013- ISMS Policy
14.	Antivirus Policy	PMSL-ISMS-PO-014- Antivirus Policy
15.	Incident Management Policy	PMSL-ISMS-PO-015- Incident Management Policy
16.	Audit Policy	PMSL-ISMS-PO-016- Audit Policy
17.	Operations Security Management policy	PMSL-ISMS-PO-017- Operations Security Management policy
18.	Communication Security Management policy	PMSL-ISMS-PO-018-Communication Security Management policy
19.	E-mail Disclaimer	PMSL-ISMS-PO-019--E-mail Disclaimer
20.	Employee Discipline Policy	PMSL-ISMS-PO-020- Employee Discipline Policy
21.	Asset Management Policy	PMSL-ISMS-PO-021- Asset Management Policy
22.	clear desk and clear screen policy	PMSL-ISMS-PO-022- clear desk and clear screen policy
23.	Acceptable Use Policy	PMSL-ISMS-PO-023- Acceptable Use Policy
24.	Change Management Policy	PMSL-ISMS-PO-024- Change Management Policy
25.	Information Data Classification	PMSL-ISMS-PO-025 Information Data Classification
26.	capacity Management Policy	PMSL-ISMS-PO-026- capacity Management Policy
27.	Induction policy	PMSL-ISMS-PO-027- Induction policy
28.	Information security Policy	PMSL-ISMS-PO-028- Information security Policy
29.	Legal Compliance Policy	PMSL-ISMS-PO-029- Legal Compliance Policy

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda



ISMS Manual

Preparation Date 15th Feb 2009

Review Date 3rd February 2022

Doc. Classification: Internal

Approval Date 3rd February 2022

Doc. No.: PMSL-ISMS-MD-001

Page 22 of 27

Ver. No. 9.0

30.	Public available information security Policy	PMSL-ISMS-PO-030- Public available information security Policy
31.	Retirement Policy	PMSL-ISMS-PO-031- Retirement Policy
32.	Grievance Redressal Policy	PMSL-ISMS-PO-032- Grievance Redressal Policy
33.	Secure System Engineering Principles Policy	PMSL-ISMS-PO-033- Secure System Engineering Principles Policy
34	Supplier security Policy	PMSL-ISMS-PO-034 -Supplier Security Policy
35	ISMS Objectives	PMSL-ISMS-PO-035-ISMS Objectives
36	Patch Management Policy	PMSL-ISMS-PO-036-Patch Management Policy
37	Data Leakage Prevention Policy	PMSL-ISMS-PO-037-Data Leakage Prevention Policy

(IV) LIST OF ISMS PROCEDURES

1	Control of documented information	PMSL-ISMS-PR-001-Control of documented information
2	Management Review Meeting Procedure	PMSL-ISMS-PR-002-Management Review Meeting Procedure
3	Internal Audit Procedure	PMSL-ISMS-PR-003-Internal Audit Procedure
4	AD Procedure	PMSL-ISMS-PR-004-AD Procedure
5	Third Party Risk Procedure	PMSL-ISMS-PR-005-Third Party Risk Procedure
6	Effectiveness of control Procedure	PMSL-ISMS-PR-006-Effectiveness of control Procedure
7	User Registration Procedure	PMSL-ISMS-PR-007-User Registration Procedure
8	Physical Access Control Procedure	PMSL-ISMS-PR-008- Physical Access Control Procedure
9	DHCP Procedure	PMSL-ISMS-PR-009-DHCP Procedure
10	Information Labeling and Handling Procedure	PMSL-ISMS-PR-010-Information Labeling and Handling Procedure

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda



PLANETCAST MEDIA SERVICES LIMITED

ISMS Manual

Preparation Date 15th Feb 2009

Review Date 3rd February 2022

Doc. Classification: Internal

Approval Date 3rd February 2022


Doc. No.: PMSL-ISMS-MD-001

Page 23 of 27

Ver. No. 9.0

11	Information Security Responsibilities Procedure	PMSL-ISMS-PR-011 -Information Security Responsibilities Procedure
12	Risk Management Procedure	PMSL-ISMS-PR-012-Risk Management Procedure
13	Corrective action Procedure	PMSL-ISMS-PR-013-Corrective action Procedure
14	UPS Procedure	PMSL-ISMS-PR-014-UPS Procedure
15	AC Procedure	PMSL-ISMS-PR-015-AC Procedure
16	Redundancy Procedure	PMSL-ISMS-PR-016-Redundancy Procedure
17	Log retention Procedure	PMSL-ISMS-PR-017-Log retention Procedure
18	Log Analysis procedure	PMSL-ISMS-PR-018-Log Analysis procedure
19	Backup and restore procedure	PMSL-ISMS-PR-019-Backup and restore procedure
20	VAPT Procedure	PMSL-ISMS-PR-020-VAPT Procedure
21	Data Retention & Disposal Procedure	PMSL-ISMS-PR-021-Data Retention & Disposal Procedure
22	CCTV Procedure	PMSL-ISMS-PR-022-CCTV Procedure
23	Teleworking Procedure	PMSL-ISMS-PR-023-Teleworking Procedure
24	BCP Procedure	PMSL-ISMS-PR-024-BCP Procedure
25	Communication Procedure	PMSL-ISMS-PR-025-Communication Procedure
26	Quality Checked procedure for star content/data	PMSL-ISMS-PR-026-Quality checked procedure for Star content/data
27	Review of user access Right	PMSL-ISMS-PR-027 Review of User Access Rights
28	Free and Open Source Software Procedure	PMSL-ISMS-PR-028 Free and Open Source Software Procedure
29	Patch Management Procedure	PMSL-ISMS-PR-029-Patch Management Procedure

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
ISMS Manual	Preparation Date 15 th Feb 2009	
	Review Date 3 rd February 2022	
Doc. Classification: Internal	Approval Date 3 rd February 2022	
Doc. No.: PMSL-ISMS-MD-001	Page 24 of 27	Ver. No. 9.0

(V) LIST OF ISMS STANDARD OPERATING PROCEDURE (SOPs)

Sr. No.	Document Description	Document Reference Number
1.	Legal Deptt.	PMSL-ISMS-SP-001-Legal Deptt.
2.	HR Deptt	PMSL-ISMS-SP-002-HR Deptt.
3.	Admin Deptt.	PMSL-ISMS-SP-003-Admin Deptt.
4.	E & M Deptt.	PMSL-ISMS-SP-004-E & M Deptt.
5.	IT Deptt.	ESC-ISMS-SP-005-IT Deptt.
6.	Hub Deptt.	PMSL-ISMS-SP-006-Hub Deptt.
7.	Star Payout Deptt.,.	PMSL-ISMS-SP-007-Star Payout Deptt.
8.	Other Payout Departments	PMSL-ISMS-SP-008-Other Payouts Deptt.
9.	Vaicom Payout	PMSL-ISMS-SP-009-Vaicom Payout
10.	NGC Payout	PMSL-ISMS-SP-010-NGC Payout

(v) LIST OF ISMS FORMS

Sr. No.	Document Description	Document Reference Number
1.	Resource allocation form	PMSL-ISMS-FO-001-Resource Allocation Form
2.	Interview Score Card	PMSL-ISMS-FO-002-Interview Score Card
3.	Reference Check Form	PMSL-ISMS-FO-003-Reference Check Form
4.	Job Application Form	PMSL-ISMS-FO-004-Job Application Form

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda



PLANETCAST MEDIA SERVICES LIMITED

ISMS Manual

Preparation Date 15th Feb 2009

Review Date 3rd February 2022

Doc. Classification: Internal

Approval Date 3rd February 2022

Doc. No.: PMSL-ISMS-MD-001

Page 25 of 27

Ver. No. 9.0

5.	Termination Letter	PMSL-ISMS-FO-005- Termination Letter
6.	Clearance report	PMSL-ISMS-FO-006- Clearance report
7.	Warning Letter	PMSL-ISMS-FO-007- Warning Letter
8.	Training attendance Sheet	PMSL-ISMS-FO-008-Training attendance Sheet
9.	Induction training - Letter	PMSL-ISMS-FO-009-Induction training - Letter
10.	Training Feedback Form	PMSL-ISMS-FO-010-Training Feedback Form
11.	Exit Interview Feedback Form	PMSL-ISMS-FO-011-Exit Interview Feedback Form
12.	Document Review Form	PMSL-ISMS-FO-012-Document Review Form
13.	Non Disclosure Agreement	PMSL-ISMS-FO-013-Non Disclosure Agreement
14.	Undertaking Form	PMSL-ISMS-FO-014- Undertaking Form
15.	Joining report	PMSL-ISMS-FO-015-Joining report
16.	Exit Check List	PMSL-ISMS-FO-016-Exit Check List
17.	Joining Check List	PMSL-ISMS-FO-017- Joining Check List
18.	Full Final settlement form	PMSL-ISMS-FO-018-Full Final settlement form
19.	Indent Form	PMSL-ISMS-FO-019-Indent Form
20.	Pre-receipt Form	PMSL-ISMS-FO-020-Pre-receipt Form
21.	Training Attendance for more than 1 day	PMSL-ISMS-FO-021-Training Attendance for more than 1 day
22.	Advance or imprest application form	PMSL-ISMS-FO-022-Advance or imprest application form
23.	Application for leave	PMSL-ISMS-FO-023-Application for leave
24.	Birthday marriage Anniversary Reimbursement claim form	PMSL-ISMS-FO-024-Birthday marriage Anniversary Reimbursement claim form

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda



PLANETCAST MEDIA SERVICES LIMITED

ISMS Manual

Preparation Date 15th Feb 2009

Review Date 3rd February 2022

Doc. Classification: Internal

Approval Date 3rd February 2022

Doc. No.: PMSL-ISMS-MD-001

Page 26 of 27

Ver. No. 9.0

25.	Conveyance claim	PMSL-ISMS-FO-025-Conveyance claim
26.	Entertainment Business Promotion expense Claim Form	PMSL-ISMS-FO-026-Entertainment Business Promotion expense Claim Form
27.	Leave travel assistance form	PMSL-ISMS-FO-027-Leave travel assistance form
28.	Local conveyance reimbursement form	PMSL-ISMS-FO-028-Local conveyance reimbursement form
29.	Medical Reimbursement form	PMSL-ISMS-FO-029-Medical Reimbursement form
30.	Official Duty	PMSL-ISMS-FO-030-Official Duty
31.	Reimbursement Claim	PMSL-ISMS-FO-031-Reimbursement Claim
32.	Request for advance or imprest Form	PMSL-ISMS-FO-032-Request for advance or imprest Form
33.	Taxi requisition Form	PMSL-ISMS-FO-033-Taxi requisition Form
34.	Tour authorization claim	PMSL-ISMS-FO-034-Tour authorization claim
35.	Ticket requisition Form	PMSL-ISMS-FO-035-Ticket requisition Form
36.	BCP Evaluation Form	PMSL-ISMS-FO-036- BCP Evaluation Form
37.	Business Continuity Test form	PMSL-ISMS-FO-037-Business Continuity Test form
38.	Corrective action Report Form	PMSL-ISMS-FO-038-Corrective action Report Form
39.	Data Center Access Form	PMSL-ISMS-FO-039-Data Center Access Form
40.	ISMS Internal audit report form	PMSL-ISMS-FO-041-ISMS Internal audit report form
41.	In-word -out word movement Form	PMSL-ISMS-FO-042-In word-out word movement Form
42.	Vendor Contact List form	PMSL-ISMS-FO-043-Vendor Contact List form
43.	Management Review Meeting Form	PMSL-ISMS-FO-044-Management Review Meeting Form

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda



PLANETCAST MEDIA SERVICES LIMITED

ISMS Manual

Preparation Date 15th Feb 2009

Review Date 3rd February 2022

Doc. Classification: Internal

Approval Date 3rd February 2022

Doc. No.: PMSL-ISMS-MD-001

Page 27 of 27

Ver. No. 9.0

44.	Fire Extinguisher Maintenance Check Sheet	PMSL-ISMS-FO-045-Fire Extinguisher Maintenance Check Sheet
45.	Backup Register Form	PMSL-ISMS-FO-048-Backup Register Form
46.	Software License Version	PMSL-ISMS-FO-049- Software License Version
47.	Backup Testing Log Form	PMSL-ISMS-FO-050- Backup Testing Log Form
48.	Backup restore form	PMSL-ISMS-FO-051-Backup restore form
49.	SLA Tracking Sheet	PMSL-ISMS-FO-052- SLA Tracking Sheet
50.	Maintainance Schedule checklist Form	PMSL-ISMS-FO-053- Maintainance Schedule checklist Form
51.	Access Matrix Form	PMSL-ISMS-FO-054-Access Matrix Form
52.	Visitor Device Details Form	PMSL-ISMS-FO-055-Visitor Device Details Form
53.	Mock Drill	PMSL-ISMS-FO-056-Mock drill
54.	Spair Equipment sheet details	PMSL-ISMS-FO-057-Spair equipment sheet details
55.	Star Report	PMSL-ISMS-FO-058-Star Report
56.	Internet user ID requisition Form	PMSL-ISMS-FO-059-Internet user ID requisition Form
57.	Application access Form	PMSL-ISMS-FO-060-Application Access Form

Prepared By	Reviewed By	Approved By
Kartikey Datta	Sanjeev Bajaj	Sanjay Duda