PLANETCAST MEDIA SERVICES LIMITED

Physical 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	N.C. Mallick	N.K. Badola	Navneet Chandra
1.0	4th Jan 2010	6th Jan 2010	-	-	N.C. Mallick	N.K.Badola
2.0	28th Dec 2011	2nd Jan 2012	-	-	Prashant Kumar	N.K.Badola
2.0	2nd Jan 2013	2nd Jan 2013	-	-	Prashant Kumar	N.K.Badola
2.0	18th March 2013	19th March 2013	-	-	Prashant Kumar	N.K.Badola
3.0	13th Jan 2014	13th Jan 2014	-	-	Prashant Kumar	N.K.Badola
3.0	8th Jan 2015	9th Jan 2015	-	-	Prashant Kumar	N.K.Badola
3.1	8th Jan 2016	9th Jan 2016	-	-	Prashant Kumar	N.K.Badola
3.1	20th March 2016	21st March 2016	-	-	Prashnat kumar	N.K.Badola
3.1	3rd March 2017	4th March 2017	-	-	Sanjeev Malick	N.K.Badola
3.1	14th February 2018	14th February 2018	-	-	Sanjeev Malick	N.K.Badola
3.1	8th February 2019	11th February 2019	-	-	Sanjeev Malick	N.K.Badola

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	Prashant Kumar
2.0	In section D, First point was deleted	Page 4	28th Dec 2011	Prashant Kumar
3.0	Point no G, H and I added	Page 4	13th Jan 2014	Prashant Kumar
3.1	Logo & Company name changed	--	20th March 2016	Prashant Kumar

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
N.K.Badola	Sr.V.P.	Admin Deptt.	3.1	Electronic	11th February 2019
Sanjay Duda	CISO	Managmeent	3.1	Electronic	11th February 2019

Physical Security Policy

1. Purpose

To prevent unauthorized physical access, damage, and interference to PMSL premises and information, and to prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

2. Scope

The policy covers the corporate office building at (PMSL C-34, Sector -62, Electronic City, Noida) and the equipment housed within the corporate office premises.

3. Policy

A. Security of the Premises:-

(i) The office building/site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions.

(ii) As per nature of the operations, suitable floor structuring, lighting, power and water damage protection requirements shall be provided.

(iii) Construction shall comply with all applicable building and safety regulations as laid down by the relevant Government agencies.

(iv) Only authorized personnel shall be permitted to take PMSL property off the premises and they shall be responsible for protecting the property and controlling its use.

(v) The work area shall be properly secured to protect both sensitive and critical information and ensure privacy. Workstations shall be placed in a location that protects the confidentiality of data. Documents and media shall be stored in a secure manner.

(vi) Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.

B. Security & Maintenance of the equipment's:-

(i) Equipment shall be cited or protected to reduce the risks from environment threats and hazards also to minimize unnecessary access into work areas.

(ii) Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All critical applications shall be configured to switch over to an alternate power source immediately upon loss of power.

(iii) Controls shall be adopted to minimize the risk of potential threats including:

1. Theft
2. Fire
3. Explosives
4. Smoke
5. Water (or supply failure)
6. Dust

7. Vibration
8. Electrical supply interference
9. Electromagnetic radiation

(iv) Equipment shall be correctly maintained to ensure its continued availability and integrity in accordance with the supplier's recommended service intervals and specifications.

(v) Records shall be maintained for all suspected or actual faults and all preventive and corrective action. Only authorized maintenance personnel shall carry out repairs and services.

(vi) Equipment and Media taken off the premises shall not be left unattended in public places. Portable computers shall be carried as hand luggage and disguised when traveling**.**

(vii) Adequate insurance cover shall be in place to protect equipment off site.

C. **Physical Access:-**

(i) Responsibilities round the clock, seven days a week, three hundred sixty five days (three sixty six days if leap year) a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.

(ii) All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.

(iii) Closed-Circuit TV (CCTV) Surveillance monitoring shall be performed to ensure workforce safety and prevent property loss. Surveillance monitoring shall be limited to areas perceived as high risk unless otherwise required.

(iv) Visitor Control shall be implemented which may include any or all of the following features:

- ✧ Visitor log maintained.
- ✧ Sign-in/sign-out procedures with time recorded.
- ✧ Temporary badge with number properly displayed and recorded.

(v) A separate devices register shall be maintained for visitors.

(vi) All visitors shall scan their baggage in the scanner and declare all items at the main gate itself

D. **Fire Protection:-**

(i) Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.

(ii) Periodic testing, inspection and maintenance of the fire equipment shall be carried out.

(ii) Smoke detectors shall be installed in all critical area, periodic testing, inspection and maintenance shall be carried out.

E. Environmental Protection:-

(i) The temperature and humidity condition in the operational site shall be monitored and controlled periodically.

(ii) Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.

(iii) Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

F. Cabling Security:-

(i) Power and Telecommunications cabling carrying data or supporting information services shall be underground or subject to adequate alternative protection.

(ii) Network cabling shall be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas.

(iii) Power cables shall be segregated from communication cable to prevent interference.

G. Removal of Assets:-

Equipment, Information, software shall not be taken off-site without prior authorization.

***H.* Unattended User Equipment:-**

User shall ensure that unattended equipment has appropriate Protection.

I. Clear Desk and Clear Screen Policy

i) Clear desk policy for papers and removable storage media.

ii) Clear screen policy for information processing facilities shall be adopted. Refer to (PMSL-ISMS-PO-022 Clear desk and clear screen policy)

***4.* Post Condition**

None

***5.* Point of Contact**

Admin Manager /E & M Deptt, PMSL.

***6.* Enforcement**

- All users shall read and abide by this Physical 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.