PLANETCAST MEDIA SERVICES LIMITED

Acceptable Use Policy

Document Release History

Version	Preparation Date	Review Date	Approval Date	Prepared By	Reviewed By	Approved By
1.0	16th Feb 2009	16th Feb 2009	15th Feb 2009	Nidhi Sharma	N.K.Badola	Navneet Chandra
2.0	4th Jan 2010	6th Jan 2010	-	-	Nidhi Sharma	N.K.Badola
3.0	28th Dec 2011	2nd Jan 2012	-	-	Karuna Parmar	N.K.Badola
3.0	2nd Jan 2013	2nd Jan 2013	-	-	Karuna Parmar	N.K.Badola
3.0	22nd March 2013	22nd March 2013	-	-	Karuna Parmar	N.K.Badola
3.1	12th Jan 2014	13th Jan 2014	-	-	Karuna Parmar	N.K.Badola
3.1	8th Jan 2015	9th Jan 2015	-	Charu Gera	Shweta Ranjan	N.K.Badola
3.2	8th Jan 2016	9th Jan 2016	-	-	Shweta Ranjan	N.K.Badola
3.3	29th March 2016	29th March 2016	-	-	Shweta Ranjan	N.K.Badola
3.3	3rd March 2017	4th March 2017	-	-	Shweta Ranjan	N.K.Badola
3.3	13th February 2018	13th February 2018	-	-	Shweta Ranjan	N.K.Badola
3.3	8th February 2019	11th February 2019	-	-	Shweta Ranjan	N.K.Badola

Document Maintenance

Version	Description of Change	Chapter / Section / Page	Date	Updated / Revised By
2.0	User level Password changed in 90 days.	Page 2	4th Jan 2010	N.K.Badola
3.0	User level Password changed in 45 days instead of 90 days.	Page4	28th Dec 2011	N.K.Badola
3.0	All PCs should be locked off with in 1 minute for any inactivity.	Page 4	28th Dec 2011	N.K.Badola
3.0	Point of contact was changed	Page 6	28th Dec 2011	N.K.Badola
3.1	First page Document control format changed.	Page 1	28th Dec 2011	N.K.Badola
3.2	Some point added in 3.2 section	Page 3	18th April 2014	N.K.Badola
3.3	Logo & Company Name changes	--	29th March 2016	N.K.Badola

Document Maintenance

Version	Document Type (Printed / Electronic)	Custodian of Document
3.3	Electronic	CISO

Document Distribution

Name	Title	Department	Version	Document Type	Approval Date
Sanjay Duda	CISO	ISMS Team	3.3	Electronic	11th February 2019

Acceptable Use Policy

1.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at PMSL. These rules are in place to protect the employee PMSL,Inappropriate use exposes PMSL to risks including virus attacks, compromise of network systems and services, and legal issues.

PMSL’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to PMSL’s established culture of openness, trust and integrity. PMSL is committed to protecting PMSL's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of PMSL. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

2.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at PMSL, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by PMSL.

3.0 Policy

3.1 General Use and Ownership

1. While PMSL’s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of PMSL. Because of the need to protect PMSL’s network, management cannot guarantee the confidentiality of information stored on any network device belonging to PMSL.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. PMSL recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within PMSL may monitor equipment, systems and network traffic at any time,Refer to-PMSL-ISMS-016 Audit policy
5. PMSL reserves the right to audit networks and systems yearly to ensure compliance with this policy.

3.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Information Classification Policy. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed 30 Days. user level passwords should be changed with in 45 Days.
3. All PCs, laptops and workstations should be secured if the user logs in through local user account by locking (control-alt-delete for Win2K users and Windows+L for other higher versions of windows) when the host will be unattended and if the user logs in through active directory account the system will be locked automatically within a minute or lock pressing (control-alt-delete for Win2K users and Windows+L for other higher versions of windows) when the host is unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect device in accordance with the “Personal communication device Policy”.
5. On all desktops USB port will be blocked.
6. All hosts used by the employee that are connected to the PMSL Internet/Intranet whether owned by the employee or PMSL, shall be continually executing approved virus-scanning software with a current virus database.
7. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

3.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of PMSL authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing PMSL-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

3.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the

installation or distribution of "pirated" or other software products that are not appropriately licensed for use by PMSL.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which PMSL Or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using an PMSL computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any PMSL account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to PMSL is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account (for example-denial of service attack).
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet.
15. Providing information about, or lists of, PMSL employees to parties outside PMSL.

3.5 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forgoing, of email header information.
4. Use of unsolicited email originating from within PMSL's networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by PMSL or connected via PMSL’s network.

4.0 Point of Contact

Sr. V.P. (HR Deptt.), PMSL.

5.0 Enforcement

- All users shall read and abide by this Acceptable Use 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.

.

6.0 Definitions

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings.