

**Password Policy**Preparation Date 15th Feb 2009

Review Date : 8th February 2019

Doc. Classification: Internal

Approval Date : 11th February 2019

Doc. No.: PMSL-ISMS-PO-005

Page 1 of 7

Ver. No 4.1

Planetcast Media Services Ltd.**Password Policy****Document Release History**

Version	Preparation Date	Review Date	Approval Date	Prepared By	Reviewed By	Approved By
1.0	16 th Feb 2009	16 th Feb 2009	15 th Feb 2009	Manish Badoni	Nutesh	Rajesh Yadvenu
2.0	4 th Jan 2010	6 th Jan 2010	-	-	Nutesh	Rajesh Yadvenu
3.0	28 th Dec 2011	2 nd Jan 2012	-	-	Rakesh Kumar	Rajesh Yadvenu
3.0	2 nd Jan 2013	2 nd Jan 2013	-	-	Rakesh Kumar	Rajesh Yadvenu
3.0	18 th March 2013	19 th March 2013	-	-	Rakesh Kumar	Rajesh Yadvenu
3.1	12 th Jan 2014	13 th Jan 2014	-	-	Rakesh Kumar	Rajesh Yadvenu
3.2	8 th Jan 2015	9 th Jan 2015	-	-	Rakesh Kumar	Rajesh Yadvenu
4.0	18 th Jan 2016	20 th Jan 2016	-	-	Rakesh Kumar	Rajesh Yadvenu
4.0	9 th March 2016	9 th March 2016	-	-	Rakesh Kumar	Sanjay Duda
4.1	28 th Dec 2016	29 th Dec 2016	-	-	Rakesh Kumar	Sanjay Duda
4.1	9 th March 2017	9 th March 2017	-	-	Rakesh Kumar	Sanjay Duda
4.1	13 th February 2018	13 th February 2018	-	-	Rakesh Kumar	Sanjay Duda
4.1	8 th February 2019	11 th February 2019	-	-	Rakesh Kumar	Sanjay Duda

Document Maintenance

Version	Description of Change	Chapter / Section / Page	Date	Updated / Revised By
2.0	User level password definition changed	Page 1	4 th Jan 2010	Nutesh
2.0	Password contains changed.	Page4	4 th Jan 2010	Nutesh
3.0	Application development standards point deleted.	Page 4	28 th Dec 2011	Rakesh Kumar
3.0	First page document control format changed.	Page 1	28 th Dec 2011	Rakesh Kumar

Prepared By Manish Badoni	Reviewed By Rakesh Kumar	Approved By Sanjay Duda
-------------------------------------	------------------------------------	-----------------------------------

**Password Policy**Preparation Date 15th Feb 2009

Review Date : 8th February 2019

Doc. Classification: Internal

Approval Date : 11th February 2019

Doc. No.: PMSL-ISMS-PO-005

Page 2 of 7

Ver. No 4.1

3.1	Minimum Password age changed.	Page 3	12 th Jan 2014	Rakesh Kumar
3.2	Password policy print screen added.	Page 4	8 th Jan 2015	Rakesh Kumar
4.0	Document format updated, latest screen shots attached	Page 5	18 th Jan 2016	Rakesh Kumar
4.1	Playout password policy defined	Page 4	28 th Dec 2016	Rakesh Kumar

Document Maintenance

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

Document Distribution

Name	Title	Department	Version	Document Type	Approval Date
Sanjay Duda	CISO	ISMS Team	4.1	Electronic	11th February 2019

Prepared By


Manish Badoni

Reviewed By

Rakesh Kumar

Approved By

Sanjay Duda

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
Password Policy	Preparation Date 15 th Feb 2009	
	Review Date : 8th February 2019	
Doc. Classification: Internal	Approval Date : 11th February 2019	
Doc. No.: PMSL-ISMS-PO-005	Page 3 of 7	Ver. No 4.1

Password Policy

1.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any PMSL facility, has access to the PMSL network, or stores any non-public PMSL information.

3.0 Policy


1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of PMSL entire corporate network. As such, all PMSL employees (including contractors and vendors with access to PMSL systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed after 30 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed after 45 days.
- Maximum password age shall be 45 days and minimum password age shall be 0 days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

Prepared By Manish Badoni	Reviewed By Rakesh Kumar	Approved By Sanjay Duda
-------------------------------------	------------------------------------	-----------------------------------

 PLANETCAST	PLANETCAST MEDIA SERVICES LIMITED	
Password Policy	Preparation Date 15 th Feb 2009	
	Review Date : 8th February 2019	
Doc. Classification: Internal	Approval Date : 11th February 2019	
Doc. No.: PMSL-ISMS-PO-005	Page 4 of 7	Ver. No 4.1

3.2 Playout Password Policy

- In Playout, All system level/ Server level password must be changed after 30 days.
- Maximum password age shall be 30 days and minimum password age shall be 3 days.
- Local user system that have system-level privileges granted through administrator account must have a unique password.

Screen shot is given below for Password policy implementation in all the Local user running systems.

3.3 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at PMSL. Some of the more common uses include: user level accounts, web accounts, email accounts, password protected operational sheets .Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than 8 characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, QWERTY, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

Prepared By Manish Badoni	Reviewed By Rakesh Kumar	Approved By Sanjay Duda
-------------------------------------	------------------------------------	-----------------------------------



Password Policy

Preparation Date 15th Feb 2009

Review Date : 8th February 2019

Doc. Classification: Internal

Approval Date : 11th February 2019

Doc. No.: PMSL-ISMS-PO-005

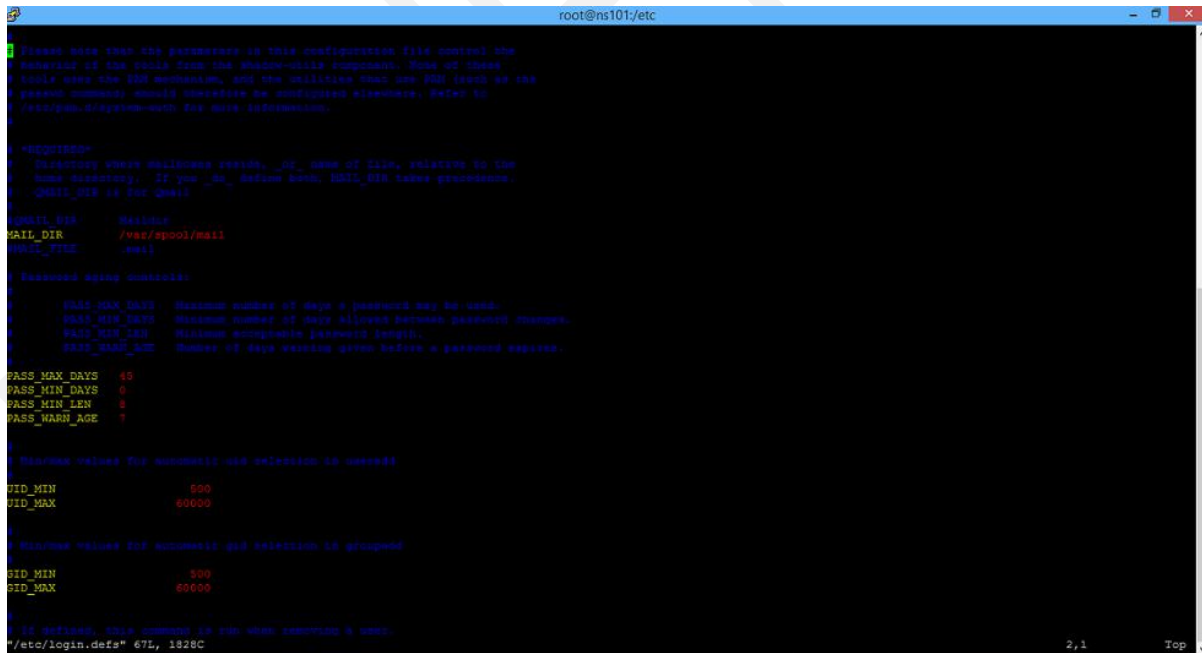
Page 5 of 7

Ver. No 4.1

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9!@#\$%^&*()_+|~- =\ {} [] : " ; ' < > ? , . /)
- Are at least 8 alphanumeric characters long and is a pass phrase (Ohmy1sturbedmyt0e).
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Screen shot is given below for Password policy implementation in all the server.



```
root@ns101:/etc
# Please note that the password in this configuration file control the
# behavior of the shells from the shadow-utils component. Some of these
# shells use the GNU libcutils, and the behavior may not be the same as the
# system default, which consists of configured libraries. Refer to
# /usr/share/doc/glibc-2.12-24/NEWS for more information.

# REQUIRE_PASS
# REQUIRE_PASS requires shadow-utils, or, some of files, existing in the
# same directory. If you do, before using PASS_MIN_DAYS take precedence.
# PASS_MIN_DAYS is for shell
#
# PASS_MIN_DAYS          Minimum
MAIL_DIR                /var/spool/mail
MAIL_FILE               mail

# Password aging controls:
#
# PASS_MAX_DAYS          Maximum number of days a password may be used.
# PASS_MIN_DAYS          Minimum number of days allowed between password changes.
# PASS_MIN_LEN           Minimum acceptable password length.
# PASS_WARN_AGE          Number of days warning given before a password expires.

PASS_MAX_DAYS          45
PASS_MIN_DAYS          0
PASS_MIN_LEN           8
PASS_WARN_AGE          7

# Minimum values for shadow-utils and shadow-utils users
#
UID_MIN                 500
UID_MAX                 60000

# Minimum values for shadow-utils and shadow-utils groups
#
GID_MIN                 500
GID_MAX                 60000

# To illustrate, this command is the same as shadow & user.
"/etc/login.defs" 67L, 1828C
```

Prepared By Manish Badoni	Reviewed By Rakesh Kumar	Approved By Sanjay Duda
-------------------------------------	------------------------------------	-----------------------------------



Password Policy

Preparation Date 15th Feb 2009

Review Date : 8th February 2019

Doc. Classification: Internal

Approval Date : 11th February 2019

Doc. No.: PMSL-ISMS-PO-005

Page 6 of 7

Ver. No 4.1

```

root@ns102:/
# Please note that the passwords in this configuration file control the
# behavior of the maild, sendmail, and shadow-utils components. Most of them
# would have the PAM mechanism, and the utilities that use PAM (such as the
# passwd command) should therefore be configured elsewhere. Refer to
# /etc/pam.d/system-auth for more information.
#
# *REQUIRED*
# Directory where mailboxes reside, or none if files, directories or the
# home directory. If you do not have mail, mail_dir takes precedence.
# (Mail_dir is for Mail)
#
MAIL_DIR          /var/spool/mail
MAIL_FILE         /var/spool/mail

# Password aging controls:
#
# PASS_MAX_DAYS   Maximum number of days a password may be used.
# PASS_MIN_DAYS   Minimum number of days allowed between password changes.
# PASS_MIN_LEN     Minimum acceptable password length.
# PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS     90
PASS_MIN_DAYS     0
PASS_MIN_LEN      8
PASS_WARN_AGE    7

# Minimum values for minimum uid selection in usersdb
#
UID_MIN           500
UID_MAX           60000

# Minimum values for minimum gid selection in groupsdb
#
GID_MIN           500
GID_MAX           60000

```

B. Password Protection Standards

Do not use the same password for PMSL accounts as for other non-PMSL access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various PMSL access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share PMSL passwords with anyone, including any of the departments like HR, Admin or IT. All passwords are to be treated as Sensitive, Confidential information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms

Prepared By Manish Badoni	Reviewed By Rakesh Kumar	Approved By Sanjay Duda
-------------------------------------	------------------------------------	-----------------------------------



Password Policy	Preparation Date 15 th Feb 2009	
	Review Date : 8th February 2019	
Doc. Classification: Internal	Approval Date : 11th February 2019	
Doc. No.: PMSL-ISMS-PO-005	Page 7 of 7	Ver. No 4.1

- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Fire fox, Explorer, Eudora, Outlook, and Netscape Messenger).

Again, do not write down passwords and store them anywhere in your office. Do not store passwords in a file on any computer system.

If an account or password is suspected to have been compromised, report the incident to the IT Dept.

C. Use of Passwords and Pass phrases for Remote Access Users

Access to the PMSL Networks via remote access is to be controlled using a public/private key system.

D. Pass phrases-

Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks."

A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good pass phrase:

"The*? #>*@TrafficOnThe101Was*&!#This Morning"

All of the rules above that apply to passwords apply to pass phrases.

4.0 Point of Contact

IT Administrator, PMSL

5.0 Enforcement

- All users shall read and abide by this Password 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.

Prepared By Manish Badoni	Reviewed By Rakesh Kumar	Approved By Sanjay Duda
-------------------------------------	------------------------------------	-----------------------------------