Maxx pharma

STANDARD OPERATING PROCEDURE

IT PASSWORD POLICY

SOP No :	GEN-D 10013	Revision :	00
SOP Type :	GENERAL SOP	Supersedes :	Nil
Format No :	SLS/QSP-001/F02.R00	Status :	Draft
Effective :	-	Expiry :	-

1.PURPOSE :

To describe the procedure for setting up individual user accounts, for granting access, to computerized laboratory instruments

2.SCOPE :

This procedure is applicable to issuance of individual user identification codes (User ID and generic password) for computerized laboratory instruments, to ensure the authenticity, integrity and confidentiality of the software generated laboratory records / data.

3. RESPONSIBILITY :

The responsibility of setting up individual user accounts lies with the Head IT/ designee

4. DEFINITION :

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. Apassword policy is often part of an organization's official regulations and may be taught as part of security awareness training.

5. PROCEDURE :

5.1 Access to computerized laboratory instruments:

5.1.1 Head IT/designee shall ensure that logical access to the computerized laboratory instruments, being used in the laboratory, is restricted to authorized personnel only.

5.1.2 Each instrument user shall be assigned an individual user identification code, for accessing the laboratory computer systems, during routine analysis. This shall ensure authenticity, integrity and confidentiality of the laboratory records generated by a user, and shall also ensure that the signer cannot readily repudiate signed record as not genuine.

5.1.3 The access/authorization shall be granted by the system administrator / lab in charge.

5.1.4 Each user identification code shall have at-least two distinct identification components namely the user name and password.

5.1.5 The identity of each individual shall be established based on the individual user ID.

5.1.6 The user name shall be unique for each individual and shall not be reused by, or reassigned to, any one else.

5.1.7 New users shall be assigned the user ID and a generic password, after a written request as in form 1, cleared by the respective heads.

5.1.8 The user ID and generic password shall be granted to a user after ascertaining that the user has adequate training / experience to generate and maintain the electronic records.

5.1.9 The user access rights and privileges for various functions shall be configured by the administrator in the laboratory workstations, based on the functions being performed / authority levels of the user.

5.1.10 User responsibilities

5.1.11 After logging in for the first time in a workstation, each user shall change the generic password given by the Administrator, in order to maintain the secrecy of his password.

5.1.12 Each user shall be accountable and responsible for actions initiated under his password usage.

5.1.13 A user shall not divulge his password to any other co-worker / analyst at any time, in order to maintain the authenticity, confidentiality and integrity of data generated under his password usage and to avoid any falsification of records.

5.2 User password policies

5.2.1 Each user password shall be at least 6 characters long, in order to avoid easy detection.

5.2.2 Each user password shall have an expiry period of 180 days, after which the user shall have to change his password, either on being prompted by the system or otherwise.

5.2.3 Each user shall be allowed a maximum of 5 attempts to login into computerized lab instrument software. After five unsuccessful attempts to log in, the user ID shall be locked by the system.

5.2.4 A warning message may be sent by the system to the administrator regarding the locking of a user ID. The user shall request in writing in the format No. SLS/QSP-040/F01 to the administrator to unlock his user ID in case of a user ID locking.

5.2.5 The administrator shall initialize / unlock the locked user ID or issue a new user ID to the concerned user, after verifying the reason thereof and documenting the same.

5.2.6 The application software's shall preferably have in-built technical controls for the transaction safeguards to prevent unauthorized use of passwords and / or identification codes and detect and report in a immediate and urgent manner any attempt at their unauthorized use to the system security unit. An evaluation shall be performed for the gap analysis. An action plan shall be prepared for up gradation / appropriate remedial action in consultation with the software vendor.

5.2.7 In case a user forgets his password or user ID, he may request (Form 1) for change of password. The administrator may give a generic password which in turn to be changed by the concerned user in his next login, after verifying the reason thereof and documenting the same.

5.2.8 The administrator shall investigate, if an attempt is made to use passwords by an unauthorized person, and take remedial action.

5.3 User accounts management

5.3.1 The names and user ID of the software users shall be recorded in a "User accounts management log book. The system / workstation number and date of issuance of user ID shall also be recorded in this logbook.

5.3.2 The logbook shall be maintained and updated regularly, by the administrator, for controlling the system access.

5.3.3 The administrator shall review the user ID list at regular intervals, to delete the obsolete users or to change the profile of a user as his role changes. Periodic changing of passwords and / or checking of identification codes for inconsistencies with current users shall also be performed during these reviews and documented in the "User accounts management log book for software's".

5.3.4 If a user is found to be involved in falsification of an electronic record, the Analytical Manager & QA Manager shall perform investigation & impact evaluation and suitable action shall be initiated.

6. REFERENCE :

21 CFR part 11

7.ENCLOSURES :

User request form format No. : SLS/QSP-040/F01

8.REVISION HISTORY :

N/A

Reason For Revision :

New SOP

Digitally Signed By :

Created By	✓	Santhosh	TRAINEE	IT	05/07/2017 12:33:09
Reviewed By	✓	Murali	MGR	AUTMN	05/07/2017 14:13:36
Approved By	☒				
Authorized By	☒				

This document is only current on the day of viewing. Printed copies are UNCONTROLLED.

------------END OF DOCUMENT------------

FORMAT-1

USER REQUEST FORM

Ref Doc No :	GEN-D 10013	Revision :	00
SOP Type :	GENERAL SOP	Supersedes :	Nil
Format No :	GEN-D 10013/F01.R00	Status :	Draft
Effective :	-	Expiry :	-

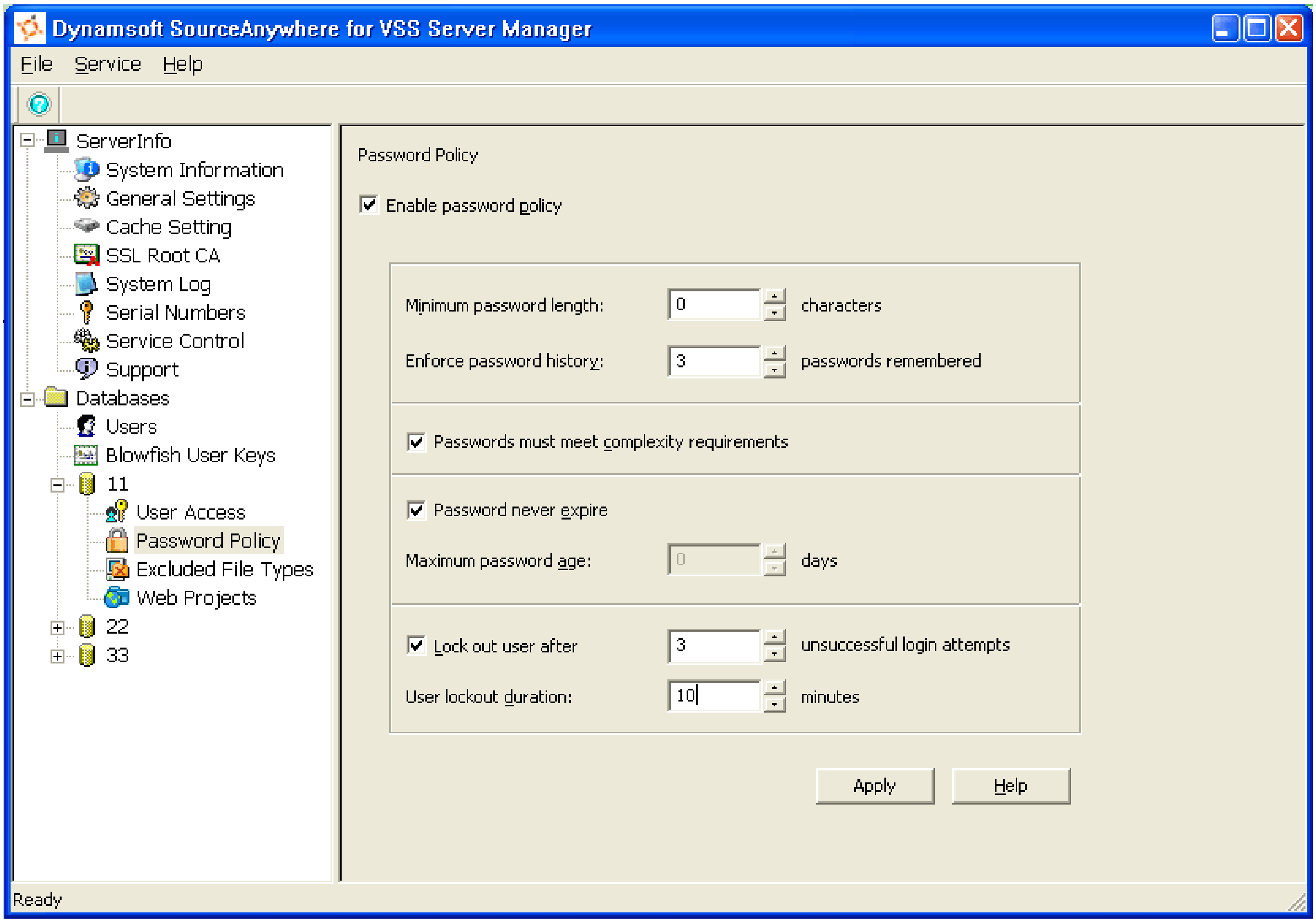
USER REQUEST FORM							Page No. of 50
S. No.	Date	User Name	Reason for request	Requested by	Reviewed by	Approved By	Remarks

SLS/QSP-040/F01.R00

ANNEXURE-1

PASSWORD SECURITY

Ref Doc No :	GEN-D 10013	Annexure No :	GEN-D 10013/A01
Revision :	00	Supersedes :	Nil
Format No :	SLS/QSP-001/F11.R00	Status :	Draft
Effective :	-	Expiry :	-



Password Policy

☑ Enable password policy

Minimum password length: 0 characters

Enforce password history: 3 passwords remembered

☑ Passwords must meet complexity requirements

☑ Password never expire

Maximum password age: 0 days

☑ Lock out user after 3 unsuccessful login attempts

User lockout duration: 10 minutes