Information Security Management System

Password Policy

TrilaSoft

AN ISO 9001 : 2008
CERTIFIED COMPANY

Document Control

Version: v1.0

Date: Dec, 2012

Author(s): TrilaSoft Solutions Pvt. Ltd.

Distribution: All

Revision History

Version #	Date	Change Highlights	Author

1.0 Introduction

This document introduces the basic concepts of software systems authentication. In particular, it focuses on the use of passwords to verify the identity of users and authenticate their access rights. Various strategies for selecting strong, hard-to-guess passwords are then discussed.

Passwords are an important aspect of computer security. A poorly chosen password may result inunauthorized access and/or exploitation of TrilaSoft'sresources and/or clients' interest. All users with access to TrilaSoft systems and RedSkysoftwaresystem, are responsible for taking the appropriate steps, asoutlined below, to select and secure their passwords.

2.0 Purpose

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

3.0 Scope

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

4.0 Policy

4.1 General

- All **system-level** passwords (e.g., Serverroot, Windows Administrator, Application level administrationaccounts, etc.) must be changed on at least on quarterly basis under normal circumstances.

- All **user-level** passwords (e.g., E-mail, Windows User, etc.) must be changed at least on quarterly basis under normal circumstances.

- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. Password Construction Guidelines

All users at TrilaSoft should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain **at least six alphanumeric characters.**
- Contain **at least three** of the five following character classes:
    - Lower case characters
    - Upper case characters
    - Numbers
    - Punctuation
    - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]"<>/ etc)

Weak passwords have the following characteristics:

- The password contains less than six 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.
    - The words "TrilaSoft", or “RedSky” or any derivation.

- ✓ Birthdays and other personal information such as addresses and phone numbers.
- ✓ Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, 12345, 54321 etc.
- ✓ Any of the above spelled backwards.

Try to create passwords that can be easily remembered. One way to do this is create a password based on asong title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way ToRemember" and the password could be: "TmB1w2R!" or some other variation.

(NOTE: Do not use any examples in this document as passwords!)

B. Password Protection Guidelines

- Always use different passwords for TrilaSoft accounts from other non-TrilaSoft access (e.g., personal ISP account, your online shopping accounts, insurance policy accounts, bank accounts etc.).

- Do not share TrilaSoft passwords with any non-TrilaSoft personnel.

- All passwords are to be treated as sensitive and confidential TrilaSoft information.

- Passwords should never be written down or stored on-line without encryption.

- Do not reveal a password in email, chat, or other electronic communication.

- Do not speak about a password in front of others.

- Do not hint at the format of a password.

- Do not reveal a password on questionnaires or security forms
- If someone demands a password, inform them about information security and password policy and direct them to the InformationSecurity Control Representatives.
- If an account or password compromise is suspected, report the incident to the Information SecurityControl Representatives.

C.Application Development Standards

Applications

- Shall support authentication of individual users.
- Shall not store passwords in clear text or in any easily reversible form.

D. Use of Passwords for RemoteAccess Users

- Access to the TrilaSoft Networks/Servers via remote access is to be controlled using password authentication for each time login is tried.

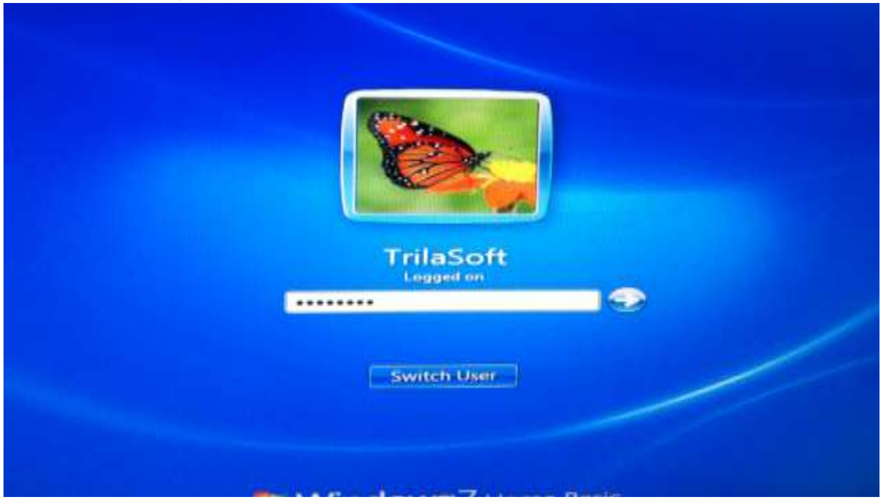
5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action. Password cracking or guessing may be performed on a periodic or random basis by the Information Security Control representatives. If a password is guessed or cracked during these exercises, the user/owner will be required to change it immediately.

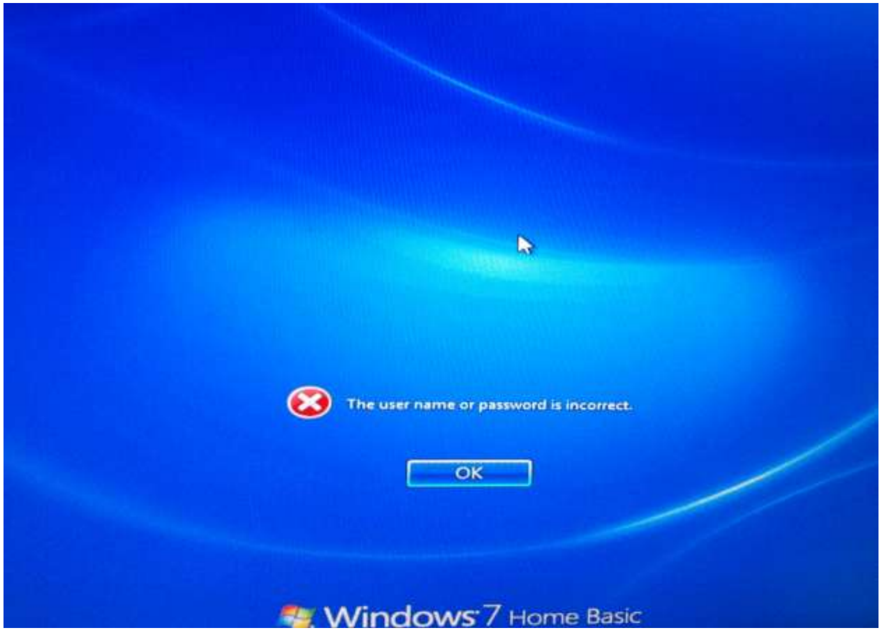
6.0 Appendix

The following screen shots gives how password mechanism is enforced within the parameters of Operating System.

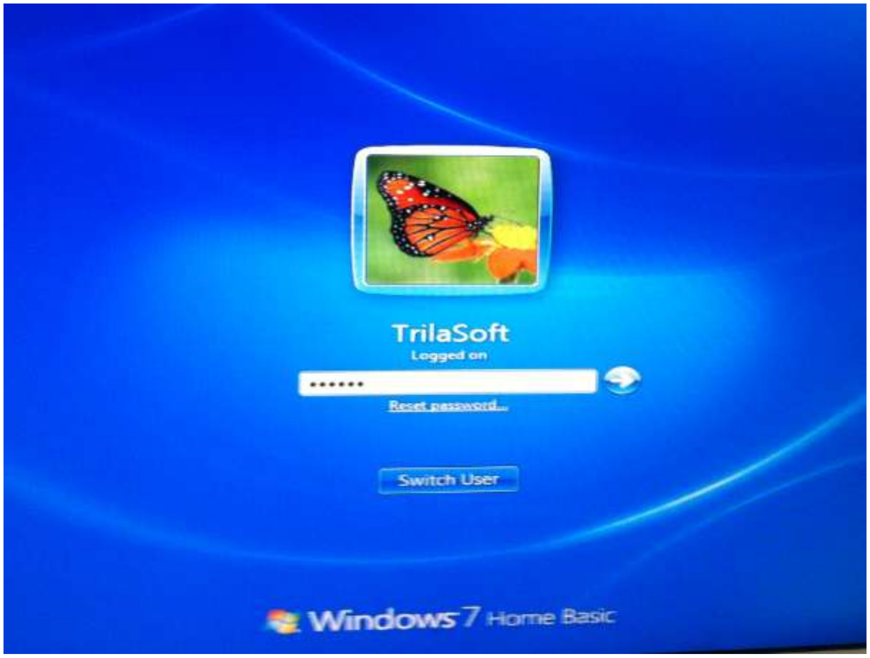
Pic-1 (wrong password entered)



Pic-2 (password validated and denied access)


The user name or password is incorrect.

Pic-3 (correct password entered)



Pic-4 (password validated and user allowed logging in)