Password Management Guidelines

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to describe the guidelines to be followed while managing user passwords. The basic means of access control to applications, networks and platforms (i.e. laptops, routers, servers, etc.) is the identification and authentication of the requesting entity. This access control is accomplished through the use of a logon account consisting of an ID and an associated password to ensure the requesting entity is known.

1.2 Responsibilities

Information Security Manager (ISM) along with Systems and Network Personnel is responsible to ensure the implementation of this procedure.

This standard is followed by all associates, contractors and consultants who access Sybrid's infrastructure.

2 Guidelines

2.1 User Password Management Guidelines

1. Individual domain user account IDs are to be constructed from the individual's first and last name seperated by a period (.). This is done for each new associate by IT. HR is responsible to request for the account creation and IT creates the account.
2. The maximum password age for user accounts is 120 days, providing that the 8 character password requirement is adhered to.
3. For domain and application accounts (that can adhere to this setting), cannot feasibly use a minimum day limit for password reuse control, selection of prior passwords is prohibited for 6 cycles.
4. For non-domain accounts and applications that cannot feasibly use a minimum day limit for password reuse control, selection of prior passwords is prohibited for 4 cycles.
5. Passwords are not permitted to be "blank" or "null" and must be constructed based on the following rules:
    a. Minimum size of a normal user account password is 8 characters and it must include at least one non-alphabetic character.

b. Minimum password length for individual accounts with elevated privileges or accounts in privileged groups (e.g. Domain Administrator, Product Support, etc.) On Windows systems is 12 characters, and UNIX systems (e.g. Root) are required to be 8 characters. Group shared accounts, system/service accounts, and Application or Database Support accounts are to adhere to the 14 character requirement when it is technically feasible and resource justified.

6. If passwords are written, they must be stored in a secure locked place, and separate from the associated logon IDs and/or application names. Other than shared support accounts and user accounts with no ability to modify financial data that are established by management for support or operational purposes, passwords must not be shared among users and are classified as PRIVATE & CONFIDENTIAL (RESTRICTED) information.
7. Passwords must not be readable on a CRT screen as they are typed or displayed in printed reports or logs.
8. Password phrases must be encrypted when electronically stored and be known in plain text only by the owner.
9. When the associates are granted access to the customer systems, its their responsibility to ensure that they use hard to guess passwords on client systems. The rules that are enforced for system passwords are applicable on client systems too.