Smartlink Network Systems Ltd.	
Document Title	Password Policy
Document Version	1.5
Document Approval Date	19th November 2010
Document Effective Date	31st December 2010
Document Last Updated Date	16th May 2012

Password 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 Smartlink's entire corporate network. As such, all Smartlink employees (including contractors and vendors with access to Smartlink systems) are responsible for taking the appropriate steps, as outlined 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 those passwords, 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 of access that supports or requires a password) on any system that resides at any Smartlink facility, has access to the Smartlink network, or stores any non-public Smartlink information. It is the responsibility of all Smartlink employees to strictly follow these guidelines.

Shared email accounts are used in specific cases (eg. rma-delhi, tech.support@digisol.com) based on business requirements. Such accounts are associated with specific Smartlink employee or group of employees. The responsibility of maintaining password security in such cases lies with the group of employees collectively and individually.

4.0 Policy
4.1 General

- Password should be at least seven characters long. (Nine characters are recommended.)

- **IT System-level passwords:**
  - Designated system-level passwords (e.g., application administration accounts, NT admin etc.) which are crucial for IT security is recommended to be changed on at least a quarterly basis by respective operational/functional teams. (Designated system-level accounts are identified in the document “Smartlink Controlled System Accounts”.) (4 times in a year)
  - Minimum 9 characters in length.
  - Password is recommended to contain any three of following four categories -
    I. Uppercase characters (A, B, C .... Z)
    II. Lowercase characters (a, b, c .... z)
    III. Digits (0, 1,2, 3, 4, 5, 6, 7, 8, 9)
    IV. Special symbols (` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . /)

- **User-level passwords:**

- PC Passwords should be changed every four months. (3 times in a year)
- Minimum 7 characters in length.
- 12 Old passwords cannot be re-used. (for PCs)
- Screensaver lockout time shall be 10mins or less. (for PCs)
- System shall lockout for 10mins after three invalid password attempts. (for PCs)
- Must contain **any three** of following four categories -
    a) Uppercase characters (A, B, C .... Z)
    b) Lowercase characters (a, b, c .... z)
    c) Digits (0, 1,2, 3, 4, 5, 6, 7, 8, 9)
    d) Special symbols (` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . /)
- Must not contain your PC Logon username or parts of your full name.

How to construct Password with: - Two simple words

Four password combinations are shown with two simple words (using above four categories)

Example: 1- word '**Hitch' 'cock'**:

1) Hitch5cock (Uppercase, digit, lowercase)
2) Hitch@cock (Uppercase, special character, lowercase)
3) hitchcock5# (lowercase, digit, special character)
4) *HITCHCOCK4 (special character, Uppercase, digit)

Example: 2 Or have a look at how most simple words can meet above password requirements –

- h,489at -- (hat)
- p*26ole -- (pole)
- Kite!31 -- (Kite)
- Bell459 -- (Bell)

Note: Do not use either of these examples as your 'active passwords'. These are for demonstration purposes only.

==========

- Other user-level passwords (e.g., email, web, etc.) are recommended to be changed every four months with above mentioned guidelines.
- It is the responsibility of every employee to ensure that they change the default assigned password generated during account creation.
- Every Server owner/ functional/operational team is responsible for maintaining their application/system/software/ server OS based password security as per the guidelines mentioned in this policy.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Smartlink. Some of the more common uses include: user level accounts, web accounts, email accounts and router logins. Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than 6 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 "Smartlink", "sanjose", "sanfran" or any derivation.
- 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:

- 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 seven characters long and is a passphrase (Oh1stb0). Nine characters is recommended.
- 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 without Master password /encryption protection systems. 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!

B. Password Protection Standards
Do not use the same password for Smartlink accounts as for other non-Smartlink access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Smartlink access needs. For example, select one password for the Engineering systems and a separate password for IT systems.

It is recommended not to share Smartlink passwords as it has to be treated as sensitive, Confidential Smartlink information.

Sharing password with IT staff is also not recommended. As an exception, during an IT support call, in case it is necessary to share the password with Smartlink IT staff, please ensure you change the password as soon as the work is completed by the IT staff. The responsibility of changing the password rests with the employee.

When a new employee joins or a new account is created for any system, a non-default specifically generated password is sent by IT department to the employee. This password may be sent by email to the employee or his/her reporting manager. This initial password should be changed immediately by the employee.

Here is a list of "dont's":

- Don't reveal a password over the phone to any unauthorized person.
- 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.
- 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 IT Department.

It is recommended not to use the "Remember Password" feature of applications (e.g., Email clients, IM, Web, etc)

If an account or password is suspected to have been compromised, report the incident to IT Dept immediately and change all passwords.

IT dept is authorized to perform Password cracking or guessing on random or periodic or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Use of Passwords for Remote Access Users
Access to the Smartlink Networks via remote access is recommended to be controlled using a one-time password authentication.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Revision History

Version	Date	Author	Remarks
1.0	15 th October 2009	Kiran Gole	Document created
1.0	15 th October 2009	Sandeep S	Discussed with Security Committee / Head
1.1	15 th October 2009	Kiran Gole	Document updated.
1.1	15 th October 2009	Sandeep S	Approved by Security Committee / Head
1.2	11 th November 2009	Kiran Gole	Document updated – added 4.1 (1) – password clause.
1.2	11 th November 2009	Sandeep S	Approved by Security Committee / Head
1.3	13 th November 2009	Kiran Gole	Document updated.
1.3	13 th November 2009	Sandeep S	Approved by Security Committee / Head
1.4	3 rd November 2010	Kiran Gole	Document updated.
1.4	19th November 2010	Shridhar K	Approved by Security Committee / CTO
1.5	16th May 2012	Mayur Gujar	Name & Logo updated.