Password Policy

Introduction

All staff and subcontractors who have access to Company computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

Purpose

This policy is designed to protect the Company resources on the network by requiring strong passwords along with protection of these passwords and establishing a maximum time between changes to passwords.

Scope

This policy applies to all staff and subcontractors who have any form of computer account requiring a password on the Company network including but not limited to a domain account and e-mail account.

Password Protection

Users should protect their passwords as per the following guidance:

- Avoid your passwords becoming known by never writing them down or telling anyone what they are, and be wary about letting someone see you type your password.
- Never send a password through an unencrypted email.
- Never include a password in a non-encrypted stored document.
- Never reveal your password over the telephone.
- Never hint at the format of your password.
- Never reveal or hint at your password on a form on the internet.
- Never use the "Remember Password" feature of any program.
- Never use your network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
- Report any suspicion of your password being broken to HR / SmartIT.
- If anyone asks for your password, refer them to HR / SmartIT.
- Don't use common acronyms, common words or reverse spelling of words in part of your password.
- Don't use names of people or places as part of your password.
- Don't use part of your login name in your password.
- Don't use parts of numbers easily remembered such as phone numbers or street addresses.

Password Requirements

The following password requirements will be set by SmartIT:

- Minimum Length - 8 characters
- Maximum Length - 14 characters
- Minimum complexity - passwords should use one of the following four types of characters:
    - Lowercase
    - Uppercase
    - Numbers
    - Special characters such as !@#$%^&*(){}[]
- Passwords are case sensitive
- Password history – each new password should be unique and you cannot reuse old passwords

Screen Savers

Password protected screen savers are enabled and protect the computer, and activation is within 5 minutes of user inactivity.

Computers should not be unattended with the user logged on and no password protected screen saver active.

Users should not leave computers unlocked; press the CTRL-ALT-DEL keys and select "Lock Computer".

Password Renewal

Passwords will automatically renew every 90 days and will automatically require users to rest their passwords.

Automatic renewal is supressed for field staff classification of staff as they access data through their PDA which secures data via a PIN code.

Password Reset

The threshold for accounts being locked out is 3 failed login attempts.

Where an account is locked out after 3 failed login attempts, SmartIT will need reset the account so they can check for possible break in attempts on the network.

New accounts users will log in for the first time using a password supplied by SmartIT, and will be required to reset their password straight away with one of their choosing.

Declaration

I confirm that I have read and understood this Policy and will adhere to its requirements.

Employee name:	
Employee signature:	
Date:	