Northern Ireland Ambulance Service
Health and Social Care Trust

POLICY ON THE USE AND MANAGEMENT OF PASSWORDS

Title:	Policy on the use and management of Passwords		
Purpose of Policy:	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.		
Directorate Responsible for Policy:	Finance and IT Directorate		
Name and Title of Author:	Mr Paddy Dornan, IT Manager Miss Alison Vitty, Corporate Manager		
Staff Side Consultation	HR Joint Working Group 10 September 2009. No Comments		
Equality Screened:	Yes		
Date Presented to:	ICT Steering Group	1 June 2009	
	Comments	Accepted. For management and staffside consultation	
	Trust Board	24 September 2009	
Publication Date:	01/10/2009	Review:	01/10/2012
Version:	NIAS/TW/IG/9 v1		
(01) April 2009	No previous document to supersede.		
(02)			
(03)			
(04)			

Circulation List:

This Policy was circulated to the following groups for consultation.

- Staffside (via HR Joint Working Group)
- Executive Directors and Senior Managers (during week of 1 June 2009)
-

Following approval, this policy document was circulated to the following staff and groups of staff.

- All Trust Staff
- Trust Internet/Intranet Site

Policy on the Use and Management of Passwords

1.0 Introduction

Password management is an integral aspect of computer security and information governance principles. Passwords are the front line of protection for user accounts through the Northern Ireland Ambulance Service Health and Social Care Trust.

Passwords are the primary authentication method for the Trust's IT resources and are currently employed as the basis authentication method. Passwords ensure that only authorised individuals have access to specific computer systems and establish accountability for all changes made to system resources. Badly chosen passwords endanger the information they are supposed to protect.

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

3.1 This policy applies to all staff employed within the Trust including all transient staff including trainees, secondees and professional advisors and any external contractors who are given computer accounts to access information systems owned or operated by the Trust.

3.2 Members of staff accessing computer systems should use password protection for the following:

- Domain User Accounts;
- Applications e.g access to desktop computer, CITRIX, C3, Promis, DATIX, Formic, HRMS etc
- Voice mail.

3.3 Deliberate sharing of system access passwords is a criminal offence under the Computer Misuse Act 1990. All staff are required to follow good security practices in the selection and use of passwords.

4.0 General Password Management

4.1 All privileged system level passwords e.g. root device enabled windows admin, application administration accounts must be changed on at least a quarterly basis.

4.2 All user level passwords e.g desktop computer, CITRIX, C3, Promis, DATIX, Formic, HRMS and other bespoke software systems throughout the Trust must be changed every 37 days. This is enforced by the IT Department.

4.3 Passwords must not be inserted into email messages or other forms of electronic communication.

4.4 All user level and system level passwords must conform to the guidelines stated above.

5.0 General Password Construction Guidelines

5.1 Passwords are used for various purposes throughout the Trust's day to day business operations. These include:

- Domain admin;
- Domain use;
- Application access;
- Network devices;
- Voicemail.

All Trust staff need to be aware of how to select and choose strong passwords.

Poor or weak passwords have the following characteristics:

- The password contains less than 7 characters;
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters;
  - Computer terms and names, commands, sites, companies, hardware, software;
  - Words containing the Northern Ireland Ambulance Service or Department name you work within;
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zxywvuts, 12345678 etc
  - Any of the above spelt backwards;
  - Any of the above preceded or followed by a digit (e.g. secret1, 1 secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characteristics e.g. a-z, A-Z;
- Have digits and punctuation characters as well as letters e.g. 0-9, !"@%^$*{ }/;
- Are at least 7 alphanumeric characters long and is a passphrase e.g. 0hmy1stubbedmyt0e;
- Are not a word 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 online and staff should always try to create passwords that can be easily remembered.

All Trust passwords must be at least 7 characters long and contain a mix of numeric, upper and lower case and alpha characters.

Password Protection Standards

5.2 Staff should not use the same password you have created within your day to day duties within the Trust for external usage.

5.3 Staff should not share passwords created with anyone including management. All passwords are to be treated as sensitive, confidential, Trust information.

The minimum standards for electronic passwords are as follows:

- ❖ Passwords should not be written down, emailed or spoken.
- ❖ Passwords must be kept confidential and not shared with colleagues.
- ❖ Passwords must not be blank.
- ❖ Passwords should not be typed or saved in electronic documents;
- ❖ Computer generated passwords must be changed following initial successful login.
- ❖ Passwords must not be revealed to anyone over the phone, even if the recipient is of the IT Department.
- ❖ New passwords must not bear any relation to the old. For example, if the old password is N0vember, the new password must not be N0vember1 or 1rebmev0N or any variation of N0vember.
- ❖ Once the password has been changed, the new password must be kept for 37 days before the user can be allowed to change it again.
- ❖ Passwords must be unique from previous passwords and not be recycled.
- ❖ Ensure passwords are changed when prompted.
- ❖ Change your password immediately if you have reason to believe that it has been compromised. Any such incidents should be reported to the IT Department.

If a Manager requires access to a user's account during a staff member's period of absence, leave etc, a request for access form should be sought from the IT Department. Once the form has been completed and approved by a Band 7 Manager or above, it should be forwarded for consideration to the IT Manager/Assistant IT Manager. There is not automatic right of access to a user's machine.

6.0 Policy Compliance

6.1 If any user is found to have breached this policy, they may be subject to Trust's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

7.0 Review

7.1 This policy will be reviewed every three years or at times considered necessary as a result of operational changes, legislative changes, risk assessments or when breaches in security have occurred.

Related Documentation:

This policy should be read in conjunction with:

ICT Strategy 2009/10 to 2014
ICT Security Policy
Records Management Strategy 2006-2009
Records Management Policy and associated information sheets
Data Protection Policy 2008 and associated procedures
Freedom of Information Policy 2000 and associated procedures
Email Policy
Internet Policy
Risk Management Strategy

Signed: _____

Liam McIvor (Mr)
CHIEF EXECUTIVE