iagre.org

Agriculture ■ Forestry ■ Horticulture ■ Environment ■ Amenity

IAgrE

Institution of Agricultural Engineers

Password Policy

Author **Alastair Taylor**

Approved Date **10th January 2018**

Approved by the Executive board

1. Purpose

In accordance with industry best practice, and to comply with relevant compliance regulations, the Institution of Agricultural Engineers (IAgrE) has prepared various information security policies and procedures which are intended to protect the confidentiality, integrity and availability (CIA) of their critical client data and their computing resources. This document describes the password policy at IAgrE.

2. General Password Policy

- All IAgrE information systems must require identification and authentication through passwords, pass-phrases, one-time passwords and similar password mechanisms as a minimum (a more restrictive/secure authentication mechanism is acceptable) prior to allowing user access.
- Passwords for IAgrE systems must be created in accordance with this policy and other relevant security policies.
- The IAgrE information systems (or their access control programs) must be configured (where such configuration is possible) to fulfill the requirements of this policy and other security policies.
- Passwords must be regarded as confidential information and must not be disclosed to any other person.
- Users are responsible and liable for all actions including transactions, information retrieval or communication on IAgrE information systems performed by using their user-id(s) and password(s).

3. Password Validity Policy

- All user-level passwords (e.g., application user, email, web, desktop computer, etc.) must be changed at least every 6 months.

4. User Account Lock-Out Policy

- IAgrE information systems must be configured (where this is possible) to lock the User-ID and prevent user access to the information system where an incorrect user password has been used in sequence 5 times.
- Locked Out user accounts will be reactivated within 3 business hours if using an automated reactivate system or shorter, but no less than 15 minutes. Requesting a manual reactivation may require identification of the user and determination of the reason for the lockout as a minimum for re-instating the user account and providing a new user password.

5. Password Uniqueness Policy

- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- It is recommended passwords used IAgrE accounts not be the same as passwords used for other non IAgrE access (e.g., personal ISP account, option trading, benefits, etc.).
- If possible, do not use the same password to access multiple company systems.
- Users may not reuse any of their last 8 passwords.

6. Password Communication Policy

- Passwords must not be revealed in conversations, inserted into email messages or other forms of electronic communication except for the initial password after setup.
- Passwords should not be written down, stored on any information system or storage device except in accordance with any existing company's password management procedures for safekeeping of passwords.
- Do not use the "Remember Password" feature of applications.
- If an employee either knows or suspects that his or her password has been compromised, it must be reported to the IT Department and the password changed immediately. Users can also request a new password through the automatic password reset mechanism on the application.
- The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.
- Initial passwords must be communicated to users either verbally or via encrypted email. Emails containing passwords should be deleted once they are read.
- Initial passwords should only be valid for the first log-on attempt. Users must be forced to change the password on first use.

7. Password Composition

All user-level & system-level passwords should not be easy guessed and must conform to the guidelines described below: -

- Passwords must contain 3 of the 4 following character groups:
  - A to Z
  - a to z
  - 0 to 9
  - Special Characters, i.e.! ^ $ *
- Passwords must be at least 8 characters long.
- A new password must contain at least 4 characters that are different than those found in the old password which it is replacing.
- Passwords should not be a word in any language, slang, dialect, jargon, etc.
- Passwords should not be based on personal information (such as name, birthday, address, phone number, and social security number), names of family, friends, relations, colleagues, etc.
- Passwords cannot contain all or part of your username/ID.
- Passwords must not be based on publicly known fictional characters from books, films, and so on.
- Passwords must not be based on the IAgrE name or its geographic location.
- As far as possible, passwords should be easy to remember. For this purpose, pass-phrase based passwords may be used.

For example, the phrase might be: "My House Is 7 Miles Away from Work" and the password would be: " Mhi7mafw" (NOTE: Do not use this example as your password since that would not be an intelligent choice, since this document is published to many individuals.)