farmerswife

IT SECURITY POLICY

Version:	1.1
Date of version:	25 May 2022
Created by:	Pablo Muñoz Van Reusel
Approved by:	Stephen Elliot

Change history

Date	Version	Created by	Description of change
May 2021	1.1	Michelle	updated personnel

Table of contents

1. Purpose, scope and users

The purpose of this document is to define clear rules for the use of the information system and other information assets in Farmers Wife SL.

Users of this document are all employees of Farmers Wife.

2. Basic Security Rules

2.1. Definitions

Information system – includes all servers and clients, network infrastructure, system and application software, data, and other computer subsystems and components which are owned or used by the organization or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, etc.

Information assets – in the context of this Policy, the term *information assets* is applied to information systems and other information/equipment including paper documents, mobile phones, portable computers, data storage media, etc.

2.2. Acceptable use

Information assets may be used only for business needs with the purpose of executing organization-related tasks.

2.3. Responsibility for assets

Each information asset has an owner designated in the Inventory of Assets. The asset owner is responsible for the confidentiality, integrity and availability of information in the asset in question.

2.4. Prohibited activities

It is prohibited to use information assets in a manner that unnecessarily takes up capacity, weakens the performance of the information system or poses a security threat.

2.5. Taking assets off-site

Equipment, information or software, regardless of its form or storage medium, may be taken to work off-site.

As long as said assets are outside the organization, they have to be controlled by the person who took it outside.

2.6. Return of assets upon termination of contract

Upon termination of an employment contract or other contract on the basis of which various equipment, software or information in electronic or paper form is used, the user must return all such information assets to system administrator.

2.7. Backup procedure

The user must backup all sensitive information stored on his/her computer regularly.

2.8. Antivirus protection

ESET Endpoint security must be installed on each computer with activated automatic updates.

2.9. Authorizations for information system use

Users of the information system may only access those information system assets for which they have been explicitly authorized by the asset owner.

Users may use the information system only for purposes for which they have been authorized, i.e. for which they have been granted access rights.

Users must not take part in activities which may be used to bypass information system security controls.

2.10. User account responsibilities

The user must not, directly or indirectly, allow another person to use his/her access rights, i.e. username, and must not use another person's username and/or password. The owner of the user account is its user, who is responsible for its use, and all transactions performed through this user account.

2.11. Password responsibilities

Users must apply good security practices when selecting and using passwords:

- each users shall manage their passwords to software applications with LastPass
- passwords must not be disclosed to other persons, including management and system administrators, apart from our internal local systems
- passwords must not be written down, unless a secure method has been approved by system administrator
- user-generated passwords must not be distributed through any channel (using oral, written or electronic distribution, etc.)
- passwords must be changed if there are indications that the passwords or the system may have been compromised – in that case a security incident must be reported … to whom and how?
- strong passwords must be selected, in the following way:
    - using at least 8 characters
    - using at least one numeric character

  - using at least one uppercase and at least one lowercase alphabetic character
  - using at least one special character
  - a password must not be a dictionary word, dialectal or jargon word from any language, or any of these words written backwards
  - passwords must not be based on personal data (e.g. date of birth, address, name of family member, etc.)
  - passwords must be changed every 6 months
- password must be changed at first log-on to a system
- passwords used for private purposes must not be used for business purposes

As an expiration is configured, users will be prompted to change their password on next login. When connecting via Desktop Client, the user first gets prompted to change the password and as he clicks OK, he is presented with the rules.

When connecting via Web Client, Mobile Web Client or iOS app, users will be presented with the rules after the first attempt to set a new password.

2.12. Internet use

Internet may be accessed through the organization's local network with appropriate infrastructure and firewall protection and through Direct Internet access. Hosted servers can only be accessed via VPN.

IT Manager may block access to some Internet pages for individual users, groups of users or all employees at the organization. If access to some web pages is blocked, the user may submit a written request to IT Manager for authorization to access such pages. The user must not try to bypass such restriction autonomously.

The user must regard information received through unverified websites as unreliable. Such information may be used for business purposes only after its authenticity and correctness have been verified.

The user is responsible for all possible consequences arising from unauthorized or inappropriate use of Internet services or content.

2.13. E-mail and other message exchange methods

Message exchange methods other than electronic mail also include download of files from the Internet, transfer of data via ftp, telephones, fax machines, sending SMS text messages, portable media, and forums and social networks.

IT Manager determines the communication channel that may be used for each type of data, as well as possible restrictions on who is allowed to use communication channels, i.e. defines which activities are forbidden.

Users may only send messages containing true information. It is forbidden to send materials with disturbing, unpleasant, sexually explicit, rude, slanderous or any other unacceptable or illegal content. Users must not send spam messages to persons with whom no business relationship has been established or to persons who did not require such information.

The user must save each message containing data significant for the organization's business using the method specified by IT Manager.

Each e-mail message must contain a disclaimer, except messages sent through communication systems.

2.14. Copyright

Users must not make unauthorized copies of software owned by the organization, except in cases permitted by law, by the owner or IT Manager.

Users must not copy software or other original materials from other sources, and are liable for all consequences that could arise under the intellectual property law.

3. Validity and document management

This document is valid as of 25 May 2018

The owner of this document is CEO who must check and, if necessary, update the document at least once a year.

CEO

Stephen Elliot

_____