CYBER PROTECTION POLICY

Introduction

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, FeRFA has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose

The purpose of this policy is to (a) protect FeRFA data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.

Scope

This policy applies to all of FeRFA's service providers, remote workers, permanent, and part-time employees, suppliers, and/or any individuals with access to the association's electronic systems, information, software, and/or hardware.
Confidential Data.

FeRFA defines "confidential data" as:

- Unreleased and classified financial information.
- Member, supplier, and employee information.
- Patents, business processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Association contracts and legal records.

Device Security:

Company Use

To ensure the security of all company-issued devices and information, FeRFA employees are required to:

- Keep all association-issued devices password-protected (minimum of 8 characters). This includes tablets, computers, and mobile devices.
- Secure all relevant devices before leaving their desk.
- Obtain authorisation from the Directors or CEO before removing devices from the Associations premises.
- Regularly update devices with the latest security software.

07484 075 254
support@ferfa.org.uk
2 Water Street
Stamford
Lincolnshire
PE9 2NJ
ferfa.org.uk

Personal Use

FeRFA recognises that employees may be required to use personal devices to access association systems. In these cases, employees must report this information to the Directors or CEO for record-keeping purposes. To ensure association systems are protected, all service providers and employees are required to:

- Ensure all personal devices used to access company-related systems are password protected (minimum of 8 characters).
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

Email Security

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, FeRFA requires all employees, service providers and Directors to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the IT partner regarding any suspicious emails.

Transferring Data

FeRFA recognises the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over FeRFA networks.
- Obtain the necessary authorisation from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Adhere to FeRFA data protection law and confidentiality agreement.
- Immediately alert the IT partner regarding any breaches, malicious software, and/or scams.

Disciplinary Action

Violation of this policy can lead to disciplinary action, up to and including termination. FeRFA's disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.

This policy will be reviewed periodically.

07484 075 254
support@ferfa.org.uk
2 Water Street
Stamford
Lincolnshire
PE9 2NJ
ferfa.org.uk