NORTH VIEW
Housing Association

North View is a registered Scottish charity – charity registration number SC032963

POLICY		
INFORMATION TECHNOLOGY SECURITY		
Passed:- 22/01/2025	Review Date:-	Dec-2029

1.0 Introduction

1.1 The aim of this policy is to define a clear and comprehensive security policy that outlines the rules, guidelines, and procedures for protecting the Association's IT (Information Technology) systems and data.

2.0 Purpose and Scope of this Policy

2.1 The purpose of this policy is to establish guidelines and procedures for protecting the organisation's IT systems, data, and assets from unauthorised access, misuse, and potential security breaches.

2.2 This policy aims to ensure the confidentiality, integrity, and availability of information and to promote a secure computing environment for all tenants, employees, contractors, and service users.

3.0 Security Responsibility

3.1 The Management Committee is responsible for providing the necessary resources, support, and oversight to ensure the effective implementation and enforcement of IT security measures.

3.2 The Association's external IT consultant and Maintenance Manager are responsible for implementing and maintaining appropriate security controls, monitoring systems, and responding to security incidents promptly.

3.3 All employees are responsible for adhering to this policy, following security procedures, and reporting any security incidents or concerns to the appropriate channels.

POLICY

INFORMATION TECHNOLOGY SECURITY

4.0 Access Control

4.1 User accounts are created for authorised individuals only. User access privileges will be granted based on the principle of least privilege, ensuring that users have access only to the resources necessary to perform their job responsibilities

4.2 Strong passwords will be used for all accounts, and password complexity requirements will be enforced. Passwords sharing is strictly prohibited.

5.0 Security controls

5.1 We have appropriate security controls to mitigate identified risks. This includes firewalls, intrusion detection and prevention systems, antivirus software, encryption, multi-factor authentication, and regular security updates and patches.

5.2 We ensure that our network infrastructure is properly secured by implementing secure configurations, and regularly updating and patching network devices.

5.3 We implement measures to secure endpoints such as computers and laptops, by deploying endpoint protection software, enforcing strong password policies, enabling device encryption, and regularly updating and patching endpoints.

5.4 We perform regular security assessments, including vulnerability scanning and penetration testing, to identify any weaknesses or vulnerabilities in our IT systems. This helps in proactively addressing potential security gaps and ensuring ongoing protection.

6.0 Data Protection & Equality Data

6.1 Data protection ensures the privacy of individuals by safeguarding their personal information. It helps prevent unauthorised access, use, or disclosure of sensitive data, protecting individuals from identity theft, fraud, and other privacy violations. Compliance with UK General Data Protection Regulation (UK GDPR) is crucial to avoid legal consequences, fines, and reputational damage.

6.2 This requirement includes all equality data retained by the Association. Any such information will be retained securely.

disability confident
EMPLOYER

6.3 Furthermore, the Association prohibits discriminatory or inflammatory content in any communications, including emails. The principles of the Association's Equal Opportunities and Human Rights Policy must be upheld at all times.

7.0 Training

7.1 We provide comprehensive cyber security awareness training to all employees to ensure they understand their roles and responsibilities in maintaining IT security. This includes educating them about common security threats, safe browsing practices and phishing awareness.

7.2 The Association uses a third party called Cyber Security Awareness to provide staff training. They carry out phishing exercises on a regular basis and provide ongoing cyber security awareness training.

8.0 Summary

8.1 This policy outlines the responsibilities of the Management Committee, IT consultant, Maintenance Manager and employees in maintaining IT security. It emphasises the importance of access control, including user account management and strong password practices. Additionally, it highlights the significance of data protection.

8.2 In conclusion, the implementation of a robust IT Security Policy is essential for safeguarding our organisation's IT systems, data, and assets from potential threats and security breaches. By adhering to this policy, employees, contractors, and stakeholders contribute to creating a secure IT environment that ensures the confidentiality, integrity, and availability of information.

End of Policy

reviews and amendments:-

established 26/07/2023
reviewed 22/01/2025

disability confident EMPLOYER