Glen Housing Association

I.T. SECURITY POLICY

POLICY NO. 57

Date Reviewed:	August 2025
Date of Next Review:	August 2028
Regulatory Standards of Governance and Financial Management	**RS 4:** **The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.** **Guidance: 4.3** *The governing body identifies risks that might prevent it from achieving the RSL's purpose and has effective strategies and systems for risk management and mitigation, internal control and audit* **RS 5:** **The RSL conducts its affairs with honesty and integrity** **Guidance: 5.1** *The RSL conducts its affairs with honesty and integrity and, through the actions of the governing body and staff, upholds the good reputation of the RSL and the sector.*

1. PURPOSE AND SCOPE

This policy defines the security measures required to protect Glen Housing Association's information systems, assets, and data from unauthorised access, loss, or compromise, in alignment with Cyber Essentials Plus and National Cyber Security Centre (NCSC) guidance. It applies to all staff, contractors, and third parties accessing our systems or data.

2. GOVERNANCE AND RESPONSIBILITIES

The Board of Management and all staff share responsibility for safeguarding the confidentiality, integrity, and availability of the Association's information and systems. The Corporate Manager is responsible for overseeing compliance, reporting incidents, and ensuring regular reviews

3. ACCESS CONTROL

- All staff will have unique user accounts with permissions granted on a least privilege basis.
- Access to systems and data is granted only where necessary for job roles
- Accounts must be disabled immediately upon staff departure or role change
- Passwords must:
  - Meet Microsoft 365 minimum requirements (8+ characters, three of four character types: upper, lower, number, symbol)
  - Follow NCSC guidance of three random, unrelated words
  - Be unique and never reused
- Multi-Factor Authentication (MFA) is mandatory for all remote access, admin accounts, and cloud services
- Shared accounts are prohibited unless technically unavoidable, with usage logged and monitored

4. SECURE CONFIGURATION

- All systems and devices must be configured to security best practices
- Default passwords must be changed before deployment
- Only approved software from trusted sources is permitted
- Unused services, accounts, and software must be removed or disabled

5. MALWARE PROTECTION

- ESET Endpoint Protection is deployed to all devices, configured for real-time scanning and automatic updates
- All removable media must be scanned before use
- Users must not download or install software without approval
- Phishing simulations will be conducted quarterly, with targeted training for staff where needed.

6. PATCH MANAGEMENT

- All security updates for operating systems and applications must be applied within 14 days of release
- Automated patch management tools will be used where possible
- Unsupported software and operating systems are prohibited

7. FIREWALLS AND NETWORK SECURITY

- The Ubiquiti UDM Pro firewall protects our network and is configured to block unauthorised inbound and outbound traffic
- Firewall configurations are reviewed quarterly and updated against the latest known threats
- Guest Wi-Fi networks are segregated from the corporate network

8. DATA PROTECTION AND BACKUP

- All data must be stored on company servers or approved cloud platforms with nightly backups
- The Replibit cloud backup system performs daily full backups, monitored 24/7
- Backups are tested at least twice a year to verify data integrity
- Data retention aligns with the Association’s Data Retention Policy and legal requirements

9. MOBILE DEVICE AND REMOTE WORKING SECURITY

- All laptops, tablets, and mobile phones must be encrypted, password protected, and managed via Microsoft Intune
- Lost or stolen devices must be reported immediately to the Corporate Manager for remote wiping
- Devices must not be left unattended in public spaces or vehicles

10. INCIDENT RESPONSE

- All suspected or actual security incidents must be reported immediately to the Corporate Manager
- The Disaster Recovery and Business Continuity plan will be followed, including containment, investigation, and reporting to relevant authorities (including the ICO if required)

11. EQUIPMENT DISPOSAL

- All decommissioned IT equipment will be securely wiped or physically destroyed by an approved provider, with certificates of destruction retained

12. POLICY REVIEW

This policy will be reviewed every 3 years, or earlier following any significant change in infrastructure, legislation, or best practice