INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY POLICY
(Ref: CS/04)

Purpose of Policy: The policy sets out the Association's procedures for maintaining effective ICT Security. Its rules must be followed by all staff at all times.

Policy Monitoring Details	
Department:	Corporate Services
Author:	Kathryn Miller & David Rothwell ICT Officer
Status:	Association Policy
Internally reviewed:	January 2024
Updated:	January 2024
Planned Review Date:	January 2027
Regulatory Outcomes being achieved:	**Charter**: Getting good value from rents and service charges (managing all resources effectively) **Regulatory Standards**: The RSL manages its resources to ensure its financial well-being, while maintaining rents at a level that tenants can afford.
Tenant Consultation Required:	No
Relevance to the Association's values	Committed **Agile** we endeavour to ensure that our policies are up to date and reflect best practice. **Professional** we comply with all regulatory and legislative requirements. People Focused
Equalities Impact Assessment	Not required

Content List:

1. Introduction

1.1 The aims of this policy are to: -

- Provide staff with suitable ICT for their working needs, including access to the programs and data they require.
- Prevent unauthorised access to confidential data' programs and hardware.
- Comply with GDPR
- Preserve data for subsequent use.
- Protect hardware from theft, fire, and other risks.
- Minimise the risk of introduction of unauthorised programs, data, viruses, or other risks.

To achieve these aims the following arrangements have been established and the following procedures are required and will be enforced: -

2. Partnership Arrangements:

2.1 MEHA has contracted with TSG to administer its ICT infrastructure, Microsoft 365 environment and Opera accounting software with related infrastructure.

2.2 MEHA has contracts with Microsoft to provide the Microsoft 365 services including Email and data storage in SharePoint. This is managed by TSG through Entra formerly known as Azure.

2.3 MEHA has contracts with Capita for their ONE Housing management cloud software and related infrastructure.

3. Physical Security:

3.1 The following physical restrictions are to be adhered to for equipment held in the office:

- Access to all our systems is restricted to authorised personnel only and any changes have to be authorised by the Corporate Services Director (CEO or other Directors) and communicated to TSG.
- Access to the main office is restricted by locked doors and a magnet lock / key fob system.
- The last member of staff in the office must protect the physical security of the ICT equipment by ensuring the building is secure and the building alarm is set.
- Regular testing of the fire alarm will take place.
- Visitors to the Association must not be left alone with a logged-on laptop, tablet or mobile phone. If the member of staff must leave them alone the device should be locked by pressing ctrl-alt-delete and selecting the "Lock this computer option'' when using a computer or locking the screen for a tablet or mobile.
- An asset register is maintained.

- All key software and licences will be kept in a secure location (if physical copies). Digital licences are handled by ICT partners see 2.0 Partnership Arrangements.
- De-commissioning of computer equipment will be done by a professional (internal or external), to ensure that all confidential data saved to the local drive has been removed.
- Insurance cover should be reviewed on an annual basis to ensure the replacement costs of all hardware, software, and data (mobile and office based) would be covered when necessary.
- If there were to be a catastrophic event such as a fire in the office and all the equipment were to be destroyed, please refer to the Business Continuity Policy, Plan 1.

3.2 For equipment held away from the office, the following restrictions should be adhered to:

- All MEHA equipment that is kept in a home environment should be kept secure (please refer to section 4.8 of the Homeworking Policy)
- Any mobile equipment that is kept in an unattended vehicle should be hidden from view.

4. Application Security:

4.1 The following application security measures should be adhered to at all times**.**

- Staff will be given unique user identities which allow access to the system, and are further protected by passwords, which must not be shared.
- Multifactor Authentication (MFA) is used wherever possible.
- Users will only be given access to relevant areas.
- All portable equipment is secured with a PIN number or Password. Passwords must be complex and should not be around easily guessed themes such as names, birthdays etc.
- All users must log out of the system if they leave the building or leave their device unattended.
- To allow for comfort breaks, a device can be locked, but only when in a secure environment.
- Devices should be set to require logging in after being unused for a period not exceeding 15 minutes.

5. Data Security:

5.1 Each department will ensure that controls are in place for data entry, processing, and reporting.

5.2 The Corporate Services Team is responsible for ensuring the ICT system is regularly backed up. This task is managed by our respective partners and is regularly tested to ensure data integrity.

5.3 The use of memory devices is not allowed.

5.4 Security updates are automatically handled through Microsoft Entra and managed by TSG on all devices however staff are regularly reminded that they are responsible for ensuring their equipment has been updated to the most recent security patch available.

5.5 Staff are reminded not to open links in emails that they think are suspicious and to report these to the ICT Officer/TSG as required.

6. Document Security:

6.1 As of June 2023 we have moved to Microsoft SharePoint, One Drive and Teams for our document storage. Users are restricted to access to only documents related to the day-to-day workload or documents with all user access i.e. Policies, templates.

6.2 SharePoint is also segregated into a MEHA Intranet (all user area), department, team areas or project areas. Data backup and security are all handled by Microsoft. Data is encrypted as standard with SharePoint and backups are created at the point of creation of the original file with the inclusion of version backups.

- One Drive provides a personal storage area.
- SharePoint provides a business storage area.
- Teams is a gateway to SharePoint while also providing Business software tools i.e. virtual meeting space, document collaboration functions.
- MEHA Intranet is an all-user space on SharePoint storing all user access documents.

SMT would prefer all documents to show a footer which shows the path and file name, to allow other users to track and locate any file.

6.2 Access to ONE Housing database is restricted, based on user need. ONE Housing is hosted and managed by Capita with dedicated IT and Security teams.

6.3 Access to Opera Pegasus 3 is also restricted, based on user need. Opera is hosted on Azure Virtual Desktop (AVD) hosted by Microsoft and managed by TSG.

7. Security Management:

7.1 The infrastructure is well protected by firewalls and virus protection that is kept regularly updated. A lot of the process is automatic through Microsoft and the other software suppliers. TSG coordinate and manage these features on a daily basis.

7.2 New viruses and attacks are being created constantly therefore anti-virus companies and network security companies cannot adapt/patch their software or operating system until they become aware of them. New viruses and attacks therefore continue to flourish, and users must follow the Association's procedures to protect the integrity of the system.

7.3 Penetration testing will be organised on a regular basis (every 2 years as a minimum) to ensure confidence in the network security.

7.4 Cyber Controls is a service provided by TSG (from January 2024) that will be regularly monitoring and advising us on our cyber security supplying MEHA with the following:

- Monthly Vulnerability Reports
- Yearly Audit and Action plan (including software and hardware review)
- Quarterly Cyber training
- Infrastructure patch management
- Proactive Antivirus patching
- Proactive Firewall patching

7.5 Security of the Cloud hosted services (present and future) used by MEHA is managed by our respective partners.

8. Publicising this policy:

8.1 This policy will be made available to all staff in the staff handbook.

9. Other relevant or related policies:

9.1 ICT Strategy CS/03
9.2 Acceptable Use Policy CS/05
9.3 Privacy Policy (G/24)
9.4 Homeworking Policy (HR/10) and
9.5 Business Continuity Policy (G/01)