

Introduction

This policy addresses relating to physical and cyber security issues. It complements the Data Protection elements of the Meridale Organisation's Privacy Policy and elements of the Internet / Computer Use Policy.

It is the duty of the Centre Manager to implement security procedures and to bring them to the attention of other hall users and staff when necessary.

Occasional & Regular Hall Users

At the close of each session/ letting the following security procedures should be adhered to;
Check that all external doors are locked and secure
Check that all internal doors are locked and secure
Ensure all equipment is returned to the correct cupboards and the cupboards are locked securely
After use of vacuums/ cleaning equipment should be returned to their set place

Keys

- All keys must be kept in the wall mounted key safe in the main office
- When the hall is closed, the key safe must remain locked
- All keys to offices, stores and equipment should be returned to the key safe after use
- Keys should not be left in doors, locks or on any surface

Safes

- Safes must be shut and locked when not attended
- All cash tins within safes must be kept locked
- No monies to be left loose in safes (must be packaged and labelled)
- No monies are to be left in offices or desks

Key Holders

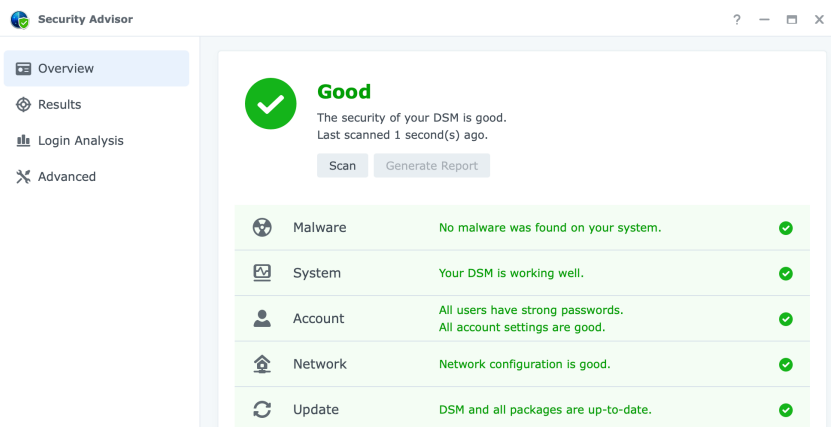
A list of designated key holders and their use privileges will be held in a secure file and kept up to date by senior members of the management team.

Equipment Inventory

A database of electrical equipment is maintained and regularly updated. All electrical equipment has been marked with the postcode. It is the duty of the Centre Manager to security mark all new equipment bought.

Cyber Security

- All Meridale PCs and laptops will run security and firewall software to protect against viruses, spyware, ransomware, leaked / hacked passwords, fake websites, unauthorised remote access/control, webcam hijacking.
- Appropriate filtering may be applied at the router to restrict access to websites via the Meridale guest wi-fi network that may present unacceptable risks.
- All PCs and laptops must be kept updated with the latest operating system updates.
- Meridale servers will be protected by a robust firewall, antivirus software, audited business class security checks for Malware, System Services, User Account Protection (permissions and password strength), Network Services and Software updates.



- Remote access to permitted files and documents stored on the Meridale server will be restricted:
 - According to role at Meridale – no access, read only, read/write
 - To using bespoke client software designed to be used in conjunction with the server operating system
 - Personal devices used for the client software must be secured with a strong unique password or by biometric means (e.g. face recognition / fingerprint)
- Server system configuration and data will be backed up daily.
- The Meridale Online Safety & Internet Use Policy will provide clear guidance for individual users

Monitoring and Review

The Trustees will review this statement periodically and no later than three years from the date below.

Signed: (On behalf of the Meridale Organisation)

Name:

Position:

Date: