# Information Security

## 1. Office Security

1.1 Office alarms - Offices at Haverfordwest have security alarms fitted. These must be operated in accordance with guidelines provided and tested weekly.

1.2 Door Security Systems: There are two systems in operation, one for the associations corridors and two for the I.T. Workroom (33) and Server Room (34).
These systems should be operated in accordance with the guidance provided.

1.3 On vacating rooms at the end of each day, staff are expected to ensure that all windows and doors are secured and locked and that blinds or curtains on the ground floor have been closed.

1.4 Computer equipment must be turned off unless requested otherwise by the ICT Officer/ICT Manager.

1.5 Procedures for dealing with visitors to the offices are to be complied with at all times with limited access to certain areas.

## 2. Hardware Protection – Workstations

2.1 Computers are to be fitted with security locks to prevent theft - each member of staff is responsible for ensuring that their machines are locked.

2.2 Portable equipment used outside of the group offices are to be used in compliance with guidelines provided by the Association.

2.3 All portable equipment is to be logged in and out by the staff member using it and an ICT Officer.

2.4 BIOS passwords should be activated for all portable computers or any workstation which holds data not stored on the computer network.

2.6 Computers should be shutdown during thunder storms to prevent damage.

## 3. Hardware Protection - Network Servers

3.1 The network servers are located a specially constructed security cabinet located in Room 34 which has it`s own door entry system.
3.2 Servers are to be protected from power failure and supply interference through the use of surge protection and battery backup systems.
3.3 In the event of power supply failure the server is to be configured to automatically close down within the time allowed by the battery backup system.
3.4 Server hardware is to be suitable to enable one server to be used to replace the other in the event of serious system failure.
3.5 Server hardware is to be covered by a maintenance SLA contract provision.
3.6 Network cabling should be installed and configured to provide minimal interruption to service in the event of component failure.
3.7 Comms Rooms have air conditioning control to keep equipment at its optimum temperature at all times.

**4. Software Protection – Network**

4.1 Passwords are to be enabled for all users who wish to access the network.

4.2 Network users are to be forced to provide unique passwords on a monthly basis.

4.3 Network configuration is to be restricted for all users except for designated administrators.

4.4 The network administrator shall restrict access to areas and directories to prevent files from being read, saved or amended by users who do not normally require such access rights.

4.5 Administration passwords are to be changed on a regular basis and not disclosed to anyone.

**5. Software Protection – General**

5.1 Where the facility to operate password protection of software exists, it should be enabled.

5.2 Installation disks should be backed up and one copy stored away from the office offsite.

5.3 All software used by the Association must be licensed according to the manufacturers rules.

5.4 No software shall be installed onto the group`s equipment without the authorisation of the ICT Officer or ICT Manager. The ICT Officer is to install any software and record it's installation and license details.

**6. Data Backup**

6.1 Data backups are to be made from the network servers on a daily basis and should include all Data/server and network settings.

6.2 All data is held on a storage unit with in the building in a sercure location only accessable to authorised ICT staff.

6.3 One copy of the data is to be stored away from the office offsite at all times in a secure location.

6.4 The use of portable disk/drive for means of storing and transporting data is not allowed .

**7. Virus Protection**

7.1 All servers and workstations are to have anti-virus software installed and enabled.

7.2 Regular updates to virus recognition data are to be installed - this should be at least weekly.

7.3 Staff who have laptop computers are to ensure that their machines are made available to the IT Officer upon request for virus updates to be installed.

7.4 E-mails are to be checked before reaching our mail server by diversion to a 3rd party virus checking system.

7.5 Anti-virus software should be enabled to check files on drives as a matter of routine.

7.6 Where there is any doubt regarding the possibility of a disk supplied to the Association having a virus, the disk should be passed to an ICT Officer for checking before it is used.

7.7 Virus software shall be configured so that all reports are made to the system administrator as well as the user. However, there is still an obligation upon staff to inform an ICT Officer and/or ICT Manager imediately a virus alert is displayed.

7.8 Periodic testing of virus defences/reports to be undertaken.

**8. Firewall**

8.1 All External Network traffic must pass threough the Checkpoint firewall system for internet and telecoms.

8.2 All security patch/updates are done by a third party support supplier as the terming in the SLA agreement.

8.3 Any addition security requirements are routed through a DMZ route to give additional security.

8.4 Internet Filtering will be activated to restrict times and access to websites that are not required for the running of the group`s business.

8.5 A system log will be held and accessed to monitor internet sites accessed, time used and to limit access to inappropriate material/sites.

**9. Software Protection - Service Providers**

9.1 Some service providers have their own security systems for their software - e.g. Girobank, Barclays, PCC Housing Register, etc. The security systems provided are to be used at all times.

Passwords must not be disclosed to anyone else or left written down.

**10. Remote Access**

10.1 Users accessing the remote systems data via VMview are defined as remote users and will be required to take all pecautions to ensure all passwords or unauthorised access to the groups systems are not compromised.

10.2 Special security measures must be in place to ensure that only authorised users are able to access the system. Measures adopted should include additional password protection and caller recognition to authenticate permitted users and data encryption to prevent unauthorised interception.

**Third Party Access**

10.1 External support that require access can only do so by an approived connection method that require a unquire username and password that will change on the next connection.

10.2 Any Access must be monitored by a member of the ICT team at all times until the access has expired.

**11. Transfers and Disposals**

11.1 Where a computer is to be transferred from one user to another an ICT Officer will be responsible for ensuring that data is transferred to the new computer and, once verified, ensure that it has been deleted from the old machine.

11.2 Where a computer is to be sold, loaned or donated outside of the Association, an ICT Officer must ensure that the hard disk has been reformatted and the operating system reloaded to minimise the risk of data recovery.

**12. Review**

12.1 This Policy was reviewed in April 2018 and will be subject to review in April 2019.