Data Security Policy

1 Key Details

* Policy prepared by: John Preston.
* Approved by board / management on: 1st March 2017
* Policy became operational on: 1st April 2017
* Next review date: 1st March 2019.

2 Introduction

The Information systems used by the Parish Giving Scheme (PGS) represent a considerable investment and are valuable assets to the Charity. The assets comprise equipment, software and data, essential to the effective and continuing operation of the PGS.

Much of the data is of a confidential nature, and it is necessary for all information systems to be protected against any events, accidental or malicious, which may put at risk the activities of the PGS or the investment in information.

This policy applies to all information systems used by, or for, the PGS. 'Information systems' include both computer-based systems and, non-computer based systems. All staff are required to adhere to this policy.

This policy is supported by the Data Protection Policy, and the Acceptable Use Policy.

3 Policy Aims

The purpose of data and information systems security is to ensure an appropriate level of: -

- Confidentiality: Information is obtained, held and disclosed lawfully and data access is confined to those with specified authority to view and/or change the data.
- Integrity: All system assets are operating according to specification and the accuracy of data is maintained.
- Availability: Systems and data are available when required and the output from it delivered to the user who needs it, when it is needed.

4 Staff Training and Awareness

This Policy should be read in conjunction with the Acceptable Use Policy regarding the acceptable use of computer systems by members of staff. Through agreeing this policy, induction and other training, PGS employees are aware of their roles and responsibilities and recognise threats such as phishing emails and malicious software.

5 Risk Analysis

In order to make the best use of resources, it is important to ensure that each information system is secured to a level appropriate to the measure of risk associated with it. A risk assessment is carried out for each of the PGS's information systems and measures put in place to ensure each system is secured to an appropriate level.

6. Physical Security

Servers are in a separate room from the systems and equipment which stores Personal Data. The systems and data is backed up overnight and stored offsite. The location of the server room and equipment is secure and alarmed.

7. Anti-virus, Firewall Protection and Intrusion Defence

Anti-virus products are in place and kept up to date. A Firewall is in place with all ports blocked.

Ports that are open are on custom ports that are not used for common services.

Files are locked down with NTFS (New Technology File System) permissions which are applied on a group basis.

8. Access controls

Each user has their own system username and password with enforced regular password changes with a limit to the number of failed login attempts.

Restricted user rights are assigned and delegated per specific role within PGS. Security settings are applied on a group/user basis to ensure users have access to all of the information that they need, whilst restricting areas that are irrelevant to their role.

Internally passwords are managed with alpha numeric requirement. Default passwords are not used. Passwords and access is cancelled immediately after a staff member leaves PGS Ltd or is absent for long periods.

A guest network is available which is separate to the PGS and Gloucester Diocesan network and they do not cross.

9. Segmentation

The web server is separate from the main file server and the central data store cannot be accessed directly through the website.

Servers are held on a SAN (storage area network) a high speed network of storage devices on a RAID (redundant array of independent disks). RAID is a data storage virtualization technology that combines multiple disk drive components into a logical unit for the purposes of data redundancy or performance improvement.

All Servers are backed up and securely held offsite for data protection and business continuity purposes.

10. Device hardening

Unused software & services are removed from devices. Software used by PGS is kept up to date.

11. Data security: (including physical data)

Personal data is:

- used fairly and lawfully for a specific purpose.
- adequate, relevant and not excessive.
- accurate, up to date and kept no longer than necessary.
- kept safe and secure and deleted when no longer required.
- not transferred outside the UK.

Additional protection is in place as follows:-

- Paper versions of forms and other personal data is scanned and forms are then shredded.
- desk tops are locked and staff adhere to a clear desk policy.

12. CARE contact database

The PGS uses the Care contacts database from NG Advanced NFP which has been used by some of the UK's largest fundraising charities for over 10 years including household names such as RSPB, WWF, Amnesty International UK, Marie Curie Cancer Care, British Legion and many others. It is relied on by these charities to securely and reliably process their monthly income.

Access to the CARE database is strictly limited to only PGS employees. The data is held in a secure Microsoft SQL database on dedicated servers professionally maintained for PGS by CIT.

Data is transferred to the Government Gateway using only encrypted connections and the Advanced Online Gift Aid Portal has successfully passed a penetration test by external independent experts.

The PGS uses the ability to restrict access to parts of the CARE system to ensure that employees have access only to the parts of the system appropriate for their role.

Version 1.2 March 2017