Catholic Diocese of Columbus

1700.0 - Technology

The use of technology has brought great efficiencies to the processing of information, communication, and work in general. However, with the introduction of technology came the introduction of risks that were not previously present.

The purpose of the policies in this section is to define methods for addressing and mitigating those risks. The following policies are in effect:

1701.0 – Environment Control

1702.0 – Security

1703.0 – Safeguards against Loss or Interruption

1704.0 – Software Policies

1705.0 – Use of Quickbooks

Catholic Diocese of Columbus

■ Policy ☐ Guideline

☐ Diocesan ☐ Parish ☐ School ■ All

1701.0 - Environment Control

The data contained in our technology system is to be considered an asset of the Diocese. This asset must be protected from accidental or intentional access or destruction.

The following policies will be followed by all entities:

At a minimum, each PC and network will be protected by
- Virus software - the virus definition and engine files will be kept current at all times
- Firewall software

In addition, each entity may choose to implement the following protective measures:
- Spam control software
- Adware control software
- Encryption software for control over financial transactions

For locations with personal computers which have wireless communication capabilities, connections should only be through a connection authorized by the Technology Administrator. All wireless communication must be established using adequate security to prevent unauthorized access to the network.

Employees should only use an e-mail account provided by the entity. This ensures that, should the employee leave the entity, critical communication is not lost. Personal use of an entity supplied e-mail account should be minimized.

Where an entity sponsored e-mail address has been set up for a ministry or auxiliary organization, the ministry or auxiliary organization should use only this e-mail address for communication related to that ministry or organization.

Diocesan entity websites should not implement blogs or chat rooms. Control of content is very difficult and the possibility of content that is not in keeping with the tenants of the Catholic Church is a risk of these types of technology.

Use of social media technology is subject to the policies set by the Office of Catholic Schools and the Chancery. These policies must be strictly followed.

Issued: May 15, 2008
Revised: June 30, 2013

Catholic Diocese of Columbus

■ Policy ☐ Guideline

☐ Diocesan ☐ Parish ☐ School ■ All

1702.0 - Security

Access to critical systems and data is controlled through the use of passwords. The following policies are in effect for all entities:

- Passwords will be used to control access to all desktop, laptop and network hardware
- Passwords will be used to control access to all critical systems, including: accounting; Census; payroll; internet hosting site; e-mail; etc.
- Each entity will establish a schedule for the periodic changing of passwords by each system user, which will occur no less frequently than semi-annually
- Passwords are to be kept confidential and are not to be shared
- Passwords should be unique and not easily determinable (i.e. do not use individuals name, birthdate, etc.)

To assure continuity of work, an individual should be designated by the pastor/principal/director as the Technology Administrator for the entity. This individual will control the initial setup of ID's and passwords for individuals on all critical systems.

All personal computers will be configured with an Administrator ID and secure password. In the case of dismissal of an employee, the Technology Administrator would then have access to files on the computer.

All financial and census systems will be configured with an Administrator ID and secure password. This ID and password will be retained by the Technology Administrator and pastor/principal/director. Each authorized user will then be given their own user specific ID and password.

Issued: May 15, 2008
Revised: June 30, 2013

Catholic Diocese of Columbus

■ Policy ■ Guideline

☐ Diocesan ☐ Parish ☐ School ■ All

1703.0 - Safeguards Against Loss or Interruption

There are a number of steps that can be implemented that will reduce the likelihood that data will be lost or business interrupted due to failure of equipment, theft or failure of power.

The following policies are in effect:

Backups: backups are to be taken of all critical systems and retained in a safe and secure place. See policy 1605 for backup frequency and retention for accounting, Census and payroll systems. A written backup plan should be prepared by each entity related to other critical systems (i.e. e-mail, individual employee files, etc.)

Laptops: laptops that are taken off premises, are to be kept in the employee's possession at all times to prevent theft until it can be safely left at the employee's residence.

Passwords: passwords will be used to limit access to all data which is critical to the operation of the entity, or confidential, to only those individuals who require access in order to fulfill their job duties.

The following additional measures may be taken by an entity:

Use of an Uninterruptable Power Supply: a UPS device is recommended for use with all network servers so that if power interruption occurs, the device can be shut down in a safe manner, preventing corruption of data.

Use of RAID: Raid technology allows for the duplication of critical data to a second disk drive. Although this increases the cost of hardware, it greatly assures that, in case of the loss of a network disk drive, that full operation can be restored quickly, without loss of data.

Backup of Website – a website is a valuable asset of an entity. Regular backups are to be made of website content and the backups are to be kept in a safe and secure manner.

Issued May 15, 2008

Catholic Diocese of Columbus

■ Policy ☐ Guideline

☐ Diocesan ☐ Parish ☐ School ■ All

1704.0 - Software Policy

Licensed software is protected by the copyright laws of the United States.

It is the policy of the Diocese of Columbus that all licensed software used by a Diocesan entity is to have a valid, fully paid license. Documentation is to be retained by the entity showing the validity of each license. The terms of the associated license agreement are agreed to upon use of the software. Users of the software are to adhere to all license terms of the software that they use.

Individual employees may not add any software to their system without prior authorization of the Technology Administrator. This will ensure control of proper licensing and will reduce the risk of viruses being introduced onto a personal computer or network.

Issued May 15, 2008

Catholic Diocese of Columbus

☐ Policy ■ Guideline

☐ Diocesan ☐ Parish ☐ School ■ All

1705.0 - Use of Quickbooks

It is strongly recommended that all entities of the Diocese of Columbus use **Quickbooks** as their accounting system.

The benefits of this are:

- The entity can obtain assistance in the use of the system from the Diocesan Finance Office
- Each entity can participate with other Diocesan entities in sharing of best practices related to use of the system
- Common reporting templates can be shared between entities
- Training in the use of the system can be obtained from the Diocesan Finance Office

It is strongly recommended that a custom accounting system NOT be used due to the risk of loss of support and lack of available training.

Issued May 15, 2008