

Automation System Policy

Delaware County Board of Developmental Disabilities

DCBDD Review Date: January 20, 2011
DCBDD Resolution # 11-01-16
Effective Date: January 21, 2011
Reviewing Department IT

Overview

The Delaware County Developmental Disabilities' (DCBDD) intentions for publishing an Automation System Policy is not to impose restrictions that are contrary to the DCBDD established culture of openness and trust. The Information Systems Department is committed to protecting the DCBDD's employees, clients, providers and the agency from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet and related systems including but not limited to computer equipment, software, operating systems, printers, scanners, projectors, televisions, copiers, storage media, cell phones, PDA's, e-mail accounts and World Wide Web browsing are the property of DCBDD. These systems are to be used solely for agency purposes in the course of normal business operations and the use of DCBDD owned systems for personal or commercial purposes is strictly forbidden. All users of the automation system are responsible for seeing that these information systems contained within the automation system are used in an effective, efficient, ethical and lawful manner.

Effective security is a team effort involving the participation and support of every DCBDD employee and agency who deals with DCBDD information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. DCBDD owned equipment assigned to an employee and in the personal possession of the employee for business use (i.e., cell phone, PDA, laptop, etc.) that is lost, stolen, or damaged shall be reported immediately to the Information Systems Director. It is the sole responsibility of the employee to reimburse the DCBDD the cost of repairs or the full purchase price to replace these items should they not be repairable.

Purpose

The purpose of this policy is to outline the acceptable and unacceptable use of the automated equipment owned by the DCBDD. These rules are in place to protect the employees and the DCBDD. Inappropriate use exposes the DCBDD to risks including virus attacks, compromise of network systems and services and legal issues. If a DCBDD employee is aware of any infraction it is that employees' responsibility to inform the Information Systems Director, who will in turn investigate the violation and take appropriate action.

Scope

This policy applies to employees, consultants, providers, and other workers at the DCBDD, including all personnel affiliated with third parties who utilize the DCBDD automated systems. This policy applies to all equipment that is owned, leased, purchased by, or in the possession of the DCBDD.

Confidentiality/Security (HIPAA)

The confidentiality of any information stored, created, received or sent over the e-mail system or through Internet access cannot be guaranteed. To the extent feasible, users should therefore avoid transmitting confidential information over the e-mail system or through Internet access. If electronic protected health information about an individual with a developmental disability or other individual on whose behalf services

are sought from or provided through DCBDD or an associated agency must be so transmitted, users should avoid using the consumer's full name the name of a consumer must never appear in the subject line of an e-mail message to promote confidentiality. All e-mails created or transmitted by a user must have a "Private and Confidential" disclaimer appended to the e-mail, and all users shall verify e-mail addresses to which confidential information is to be sent prior to that transmission.

Definitions of Terms and Abbreviations Used In This Policy

Automation System.

The collective group of components, whether tangible or intangible, used for creating or accessing electronic data, information and building access.

Intranet.

The DCBDD's internal network.

Internet.

The World Wide Web.

Hardware.

Any tangible piece of equipment used for creating or accessing electronic data and information and building access.

Software.

Any intangible property used for creating or accessing electronic data and information.

PC.

Any workstation using a Microsoft operating system.

Server.

The computer, peripherals, Microsoft operating system, and other associated software, which makes up the core of the DCBDD Intranet.

ISD.

The Information Systems Director.

NWA.

The Network Administrator.

VCC.

The Virtual Communications Coordinator.

ISDPT:

The Information Systems Department.

VOIP Telephone System.

Voice-Over-Internet-Protocol, a system of hardware and software that enables people to use the internet as the transmission source.

Fax Server

A system of hardware and software which allow people to send and receive fax transmissions over the internet.

MFP:

A multi-function peripheral, in the DCBDD's case this refers to the 3 copier/printer/scanners.

Access Control System:

A web-based access control system that gives access, manages, and oversees the DCBDD's physical 21 points of entry.

Automation System Use:

It is the intent of the DCBDD to provide access to specific portions of the automated system to any associated agencies or persons for the purpose of creating and/or accessing electronic data so long as it conforms to the DCBDD's mission. This policy applies to all individuals accessing the DCBDD's automation system. Again, the use of the automation system for *personal* or *commercial* purposes is *forbidden*. All agency email is stored on servers and included in daily backups, simply for the fact that it is considered a public record. Personal email correspondence is forbidden using a DCBDD.org email address.

Hardware:

The ISDPT will procure, assign, and maintain all equipment associated with the automated system. The ISDPT will maintain a record of each piece of equipment stating the item, serial number, configuration, ownership, physical location, and user assignment. All new equipment purchases will be of the most current and cost effective technology. The ISDPT will dispose of outdated equipment using procedures established by Delaware County.

Software:

The ISDPT will procure, assign, install, manage and maintain all software associated with the automated system. The DCBDD will use standardized and task specific software as outlined in Appendix A based on user classification and position description duties. Software not listed in the appendix and not owned by the DCBDD is *not* approved and will be strictly *prohibited* from being installed on DCBDD owned automated systems. This includes, but is not limited to, games, pictures, screensavers, etc. Not only is it illegal to install software on more than one machine, but also unapproved software has a potential for infecting the automation system with viruses and other types of malicious software. The DCBDD does not condone nor will tolerate "piracy" of software. DCBDD employees having non-approved software installed on their assigned workstations are subject to disciplinary action as outlined in the DCBDD personnel manual. The ISD will endeavor to ensure all same-type software is of the same version release to eliminate compatibility problems.

Intranet:

The core of the Intranet is a series of servers located within the information systems office. The ISDPT will maintain the servers and all associated hardware and software. Workstations within the building will be attached to the servers through a system of cables, switches and routers.

Data Storage:

All DCBDD related data will be stored on the servers in the appropriate directories. Directories will be established based on a general consensus of the DCBDD administration team. It is highly recommended that data be stored in annual directories where appropriate. The effective use of directories will ensure easy file storage, retrieval, and integrity. No more than five years of data will be stored on the servers. Data older than five years will be archived and stored with an off-site storage vendor. The ISDPT is not responsible for data stored on workstations local hard drive (commonly known as the "C") drive as this data is not stored on the servers and is not in the back-up schema.

Data Backup:

The ISDPT will ensure daily backups of all data stored on the servers utilizing current storage software and robust techniques. Daily backups will be encrypted, sent via a secure Internet circuit and stored at an off-site location. The backup of data stored on individual workstations local hard drives will be the sole responsibility of the assigned user. It is highly recommended that all DCBDD related data be stored on the servers to ensure back-up integrity.

Security:

Every user that has a need to access the DCBDD Intranet will be assigned a user name and password by the ISDPT which adheres to Microsoft Server password complexity requirements. The user name of each employee will determine which directories and data each user will access. These user names will also determine what permission level the user has to each file, i.e. (create, modify, delete, or read only). The DCBDD administrative team will determine data access authorization. All laptop users will utilize a data encryption program on local hard drives which will make the hard drive useless if stolen. The DCBDD also has a series of access control card panels which allow employees to gain or restrict access to certain portion of the DCBDD. Cameras are located throughout the interior and exterior of the DCBDD and all movement is recorded to the DCBDD servers, which is then stored at the DCBDD's off-site storage location.

Virus Protection:

All workstations and the servers will have virus protection software installed as outlined in Appendix A. It is recommended that files from the Internet be downloaded only if *absolutely* necessary and these programs must be approved by the ISD *prior* to downloading. Files from other computer systems or alternative storage media, such as "thumb drives," will be scanned for viruses and malicious software by the ISDPT before being copied to the DCBDD automated system. It is the assigned user's sole responsibility to inform the ISDPT that alternative media contains data that must be scanned for malicious software.

Use of Automation System for Non-DCBDD Business:

Reference should be made to the DCBDD's policy for "Use of Copiers for Non-DCBDD Business" for any printing or copying of material from the automation system. (This specific policy is located in the DCBDD Personnel Manual.) The MFP's are also equipped with a hard drive over write procedure to ensure that any saved data on the internal hard drives are completely free from private information on a daily basis.

Internet:

The Internet is a worldwide resource containing a vast amount of information. The DCBDD has determined that this valuable tool will assist in the accomplishment of the DCBDD's mission. Therefore, the DCBDD will contract with an Internet provider for access to the Internet. The DCBDD utilizes firewalls and protocol filters that inhibit the use of websites that do not adhere to the DCBDD mission statement. All internet activity is tracked, monitored and stored on an on-going basis.

Network Etiquette:

All users must abide by the rules of proper Network Etiquette. Among the uses and activities that violate Network Etiquette and constitute a violation of this policy are the following:

- (a) Using inappropriate language, including swearing, vulgarities or other language that is suggestive, obscene, profane, abusive, belligerent, harassing, defamatory or threatening.

- (b) Using the Network to make, distribute or redistribute jokes, stories or other material that would violate DCBDD's harassment or discrimination policies, including material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, sexual orientation or other protected characteristics.
- (c) Using the Network in a manner inconsistent with the professional expectations of a DCBDD employee. When using the Network, users should remember that they are representing DCBDD each time the account is used and that they are often creating documents that may be seen by the public. Communications on the Network need not be formal, but must be professional in appearance and tone.

VOIP Telephone System:

Voice Over Internet Protocol, a system of hardware and software that enables people to use the internet as the transmission source for telephone signal. The DCBDD utilizes a ShoreTel VOIP telephony system, which is integrated with Microsoft Outlook.

Fax Server:

The DCBDD has integrated faxing into the VOIP phone system enabling senders and receivers of faxes to receive and transmit faxes from their computers.

Access Control System:

The DCBDD has an access control that uses each employees Identification badge to permit or deny access to the 21 different doors through the location.

Board Approved Software

Appendix A

ShoreTel Call Manager
DocWorker
MS Office
Calendar Creator
Windows 2003 Server
Adobe Acrobat
MS Expression
MS FrontPage
Adobe Photoshop
MS Publisher
Barracuda Client
Real VNC
Adobe Reader
Windows Vista

FaxFinder Client
Cisco VPN Client
FileMaker Pro
VM Ware Client
Windows XP
QuickTime
Toshiba Scanner Client
MS Visio
BlackBerry Client
VZO Chat
Enable
GateKeeper
Symantec Anti-Virus Client
Windows 7

Other software approved by the ISD