

Automation System Policy

Delaware County Developmental Disabilities

DCDD Review Date: June 18, 2009
DCDD Resolution # 09-06-14
Effective Date: June 19, 2009
Reviewing Department Information Systems

Overview

The Delaware County Developmental Disabilities (DCDD) intentions for publishing an Automation System Policy is not to impose restrictions that are contrary to the DCDD established culture of openness and trust. The Information Systems Department is committed to protecting the DCDD'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 DCDD. These systems are to be used solely for agency purposes in the course of normal business operations and the use of DCDD 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 DCDD employee and agency who deals with DCDD information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. DCDD 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 DCDD 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 DCDD. These rules are in place to protect the employees and the DCDD. Inappropriate use exposes the DCDD to risks including virus attacks, compromise of network systems and services and legal issues. If a DCDD 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 DCDD, including all personnel affiliated with third parties who utilize the DCDD automated systems. This policy applies to all equipment that is owned, leased, purchased by, or in the possession of the DCDD.

Confidentiality (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 DCDD 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 and information

Intranet:

The DCDD's internal network

Internet:

The World Wide Web network

Extranet:

Approved workstations that have access to the DCDD automation system via VPN

Hardware:

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

Software:

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

Workstation:

Any computer consisting of a central processing unit, monitor, keyboard and mouse.

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 DCDD Intranet.

ISD:

The Information Systems Director

ISA:

The Information Systems Assistant

ISDPT:

The Information Systems Department

Automation System Use:

It is the intent of the DCDD 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 DCDD's mission. This policy applies to all individuals accessing the DCDD'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 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 DCDD 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 DCDD is *not* approved and will be strictly *prohibited* from being installed on DCDD 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 DCDD does not condone nor will tolerate "piracy" of software. DCDD employees having non-approved software installed on their assigned workstations are subject to disciplinary action as outlined in the DCDD 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 DCDD related data will be stored on the servers in the appropriate directories. Directories will be established based on a general consensus of the DCDD 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 DCDD related data be stored on the servers to ensure back-up integrity.

Security:

Every user that has a need to access the DCDD 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 DCDD 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.

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 DCDD 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-DCDD Business:

Reference should be made to the DCDD’s policy for “Use of Copiers for Non-DCDD Business” for any printing or copying of material from the automation system. (This specific policy is located in the DCDD Personnel Manual.)

Internet:

The Internet is a worldwide resource containing a vast amount of information. The DCDD has determined that this valuable tool will assist in the accomplishment of the DCDD’s mission. Therefore, the DCDD will contract with an Internet provider for access to the Internet. The DCDD utilizes firewalls and protocol filters that inhibit the use of websites that do not adhere to the DCDD 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 DCDD'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 DCDD employee. When using the Network, users should remember that they are representing DCDD 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.

Board Approved Software

Appendix A

Windows XP	Scansoft PDF Converter	Boardmaker
Windows Vista	Powerquest Lost and Found	Google Maps
MS Office XP/2003/2007 STD Pro	Norton Ghost	Yahoo Maps
GateKeeper	Enable	MapQuest
Symantec Antivirus Enterprise Edition	VZO Chat	MS Publisher
FileMaker Pro 8.5	Norton Partition Magic	
DocWorker	Cisco VPN Client	
Calendar Creator	VM Ware Client	
Windows 2003 Server	Spice Works	
Adobe Acrobat	Quicktime	
MS Expression	Kyocera Scanner Client	
MS FrontPage	MS Visio	
Adobe Photoshop	BlackBerry Client	
SPSS	Palm Treo Client	
Scansoft Paperport	Barracuda Client	
Pocketmirror	WinPak Pro Client	
Adobe Reader	Real VNC	
WireShark	MS Streets and Maps	

Other software approved by the ISD