



Series: Information Technology COA: RPM 6.01, 6.03, 8.01, 8.02
CFOP:
CFR45, CFR 164.310(d)(2)(i),
164.310(d)(2)(ii)

Procedure Name: Removable Media Use & Management
Procedure Number: IT-802
Revision #/Date: (2) / 6-1-09
Effective Date: 12/12/08

Applicable to: All CBCB employees, providers, contractors, freelancers, and other agents accessing the CBCB information network.

SUBJECT: Use and Management of Removable Media

PURPOSE:

The purpose of this procedure is to define standards, and restrictions for end-users who have legitimate business requirements to use portable or removable media on any equipment connected to the Community Based Care of Brevard's (CBCB) internal network(s), infrastructure, or related technology resources.

PROCEDURE:

Reference

CBCB Policies/Procedures: GOV-202, GOV-203, OP-1050

Removable Media Defined

Removable media (RM) is considered, but is not limited to, all devices and accompanying media that meet the following classifications:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.
- Memory cards in SD, Compact Flash, Memory Stick or any related flash-based supplemental storage media.
- USB card readers that allow connectivity to a PC.
- Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support mass data storage.
- PDAs, cell phone handsets and smart phones with internal flash or hard drive-based memory that support mass data storage.

- Digital cameras with internal or external memory support which are being used as mass storage devices. (Digital cameras are to be used for pictures ONLY.)
- Removable optical media, such as writable and rewritable DVDs, CDs, and floppy disks.
- Removable magnetic media, such as floppy drives or portable hard drives.
- Any hardware that provides connectivity through wireless means such as (WiFi, WiMAX, IrDA, Bluetooth, etc)
- Wired network access through USB, Category 5, serial, modem, etc.
- Any hardware and related software that could be used to access corporate resources.

Range of Threats When Using RMs

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive corporate data is deliberately stolen and sold by an employee.
Copyright	Software copied onto portable memory device could violate licensing.
Spyware	Spyware or tracking code enters the network via memory media.
Malware	Viruses, Trojans, Worms and other threats could be introduced via external media.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various entities.

Security Responsibilities

Securing access to and ensuring availability of corporate data is the responsibility of the CBCB Information and Technology Department (IT) under the management of the Network Administrator.

Securing the integrity of corporate data is the responsibility of the CBCB Quality & Fidelity Department under the management of the Chief Operating Officer or designee.

All CBCB staff, providers, contractors or others with access to Agency documents and the network have the responsibility to act in accordance with company policies and procedures.

Authorized Users of RMs

Access to RMs will be based on the need to perform duties apart from the conventional storage infrastructure.

CBCB Authorized Staff:

- a. Chief Executive Officer (CEO)
- b. Chief Operating Officer (COO)
- c. Chief Financial Officer (CFO)
- d. Chief Personnel & Administrative Officer (CPAO)

- e. Chief Compliance & Utilization Management Officer (CO)
- f. Public Relations (PR) Staff; i.e. Director of Development, PR Coordinator, & Other PR positions as designated by the CEO.
- g. Executive Assistant
- h. Network Administrator
- i. Director of Wraparound & Utilization Management
- j. Business Manager
- k. IT Staff as necessary and approved by the Network Administrator.
- l. Training Staff; i.e. Training Manager, Training Specialists, and the North Care Center Manager, other staff who provide regular training
- m. Administrative Assistant to the CFO
- n. Behavioral Analyst
- o. Grant Writer
- p. IT Contractor as approved by the CFO.
- q. Client Relations Specialist

Authorized Provider Staff Stationed at CBCB Facilities:

- r. Case Management Agency (CMA) Program Director
- s. CMA Lead Care Manager
- t. CMA Supervisor
- u. CMA Administrative Assistants will only be approved to use digital cameras as defined above.

Visitors & Others:

Where it is necessary for a vendor, guest, or other agent to bring data into CBCB for reasons such as presentation, training, or other such requirement, it is preferred by CBCB that such data be brought in on optical read-only media such as CD or DVD. This ensures a read-only environment which prevents inadvertent data transfer onto a portable rewritable device. Should it be impossible for the data being transported in to CBCB to be on optical media, it shall be incumbent upon the employee host of the agent to exercise prudence in the scheduling, availability and security of the computer authorized to connect the non-CBCB portable device.

Use of RMs

It is the responsibility of any CBCB staff, contractor or others who are connecting a RM to the organizational network to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. Accordingly, the following network rules will be observed:

1. IT will limit, by physical and non-physical means, the ability to connect RMs to corporate and corporate-connected infrastructure.
2. All RMs must be supplied and managed by IT. In managing the RMs, IT will document the chain of custody to include the CBCB staff, contractor or other individual acting as custodian of the RM and the intended use of the device. Authorized users will sign out the RM and date of intended return or intention for ongoing use will be documented.

- a. IT will assign and record the original password to the device. Users are not to change the password in order to allow IT to support and or recover data stored (IT CANNOT recover data from any RM without the original assigned password.)
 - b. Users are not to share their password outside IT.
3. IT will issue USB RM's as a large capacity (hard drive) for on-going administrative purposes or as smaller capacity (flash drive) for presentations and similar business use.
4. Personal owned "BlackBerry" devices (PDA) on the CBCB BlackBerry Enterprise Server fall under the control of CBCB for the purposes of enforcing this procedure. The PDAs which are used on the CBCB BlackBerry Enterprise Server shall be set to automatically lock after a 10 minute period of inactivity. All PDAs are to serve as a communication device (voice and email) and are not to be used on the CBCB Network as an RM.
5. All authorized users of RMs will physically secure all such devices used for this activity whether or not they are actually in use and/or being carried. Reasonable physical security will include but not be limited to: keeping the device out of plain sight, carrying the device on or near one's person, locking the vehicle, office, or home where the device is stored or transported, etc.
6. All RMs will contain an encrypted area requiring a password to open, except as otherwise noted. All data stored on the RM will be contained in this area. The CEO may have a RM with a non-encrypted area. However, no confidential child or family data is allowed to be placed on the non-encrypted RM.
7. CBCB staff, contractors, or others will not make modifications of any kind to company-owned and installed hardware or software and will not by-pass encryption measures. This includes, but is not limited to: reconfiguration of USB ports, installation of CD/DVD burning devices, other data management software, or non-use of the encrypted area.
8. IT will restrict the use of Universal Plug and Play on any client PCs that do not require such access for performance of duties. IT will disable CD write/re-write on PCs not required for use by the end user.
9. The CEO may summarily ban the use of all RMs at any time (emergency provision). Protection of confidential data is the highest priority.
10. IT will limit the ability of authorized users to transfer data to and from specific RMs on the enterprise network according to their specified needs.
11. IT will inventory all RMs periodically to ensure they are still in the possession of the authorized users to which they were issued, are still in working order, and are still being used for the purpose intended. A user can retain the RM for any period of time as is appropriate and required. IT may at this time inspect the device to ensure all data is stored in the encrypted area.
12. Authorized users and/or their supervisors must inform IT of any change in a user's role which would require the device(s) issued to be returned to IT. This includes but is not limited to: a change in position, a change in duties, or termination.

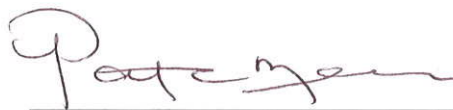
13. The authorized user agrees to and accepts that his or her use of an RM on CBCB's networks may be monitored to record dates, times, duration of access, files accessed, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains CBCB's highest priority.
14. The authorized user agrees to immediately report to his/her manager and to IT any incident or suspected incidents of unauthorized data access, data loss and/or disclosure of company resources, databases, networks, etc. This would include loss, theft (for which a police report should be filed), or any other circumstance in which company data or property may have been compromised. CBCB Security Incident Reporting procedures should be followed.
15. Upon return of an RM to be made available for redistribution, IT will perform a complete scrub of all data on the RM and prepare the media for the next user. If the RM is no longer usable, the device will be physically destroyed as outlined in procedure RM-504, Records Retention and Destruction.

Procedure Non-Compliance

Failure to comply with this procedure, in the sole discretion of the Agency, may result in the suspension of any or all technology use and connectivity privileges, disciplinary action up to and including termination; or, in the case of a contractual relationship, termination of the Agreement or Contract.

Upon learning of any failure to comply with this procedure, the Network Administrator shall report the finding to the CFO. The CFO will coordinate with appropriate CBCB Executive Management to immediately report the situation. Based on the infraction and user, the situation may be addressed by the Compliance Committee or members of Executive Management in the sole judgment of the Executive Management team.

BY DIRECTION OF THE CHIEF EXECUTIVE OFFICER:



DR. PATRICIA NELLIUS-GUTHRIE
Chief Executive Officer
CBC of Brevard, Inc.

APPROVAL DATE: 6/11/09