DOCUMENT: Policy	DOCUMENT NUMBER: IT-0521	REVISION: Original	PAGE 1 OF 4
SUBJECT: Jump Drives		EFFECTIVE DATE: 04/13/06	
OFFICE OF MIS:	DATE:		
DEPUTY SECRETARY FOR ADMINISTRATION:	DATE:		

1.0 PURPOSE

Jump drives are a convenient method for transferring data between a desktop computer and a laptop. Users can utilize jump drives in place of a floppy disk, zip drive, or CD to transfer data to another computer using a Universal Serial Bus (USB) port.

This policy outlines acceptable use, security requirements, and confidentiality issues related to the utilization of Office of Management Information Services (OMIS)-approved jump drives.

2.0 SCOPE

This policy applies to Equipment Coordinators (ECs), Regional Technicians, Regional Trainers, and all other employees who install and/or utilize OMIS-approved jump drives on DHHR laptops.

3.0 APPLICABLE DOCUMENTS/MATERIALS

3.1 In instances where state and federal laws and regulations are more restrictive than DHHR IT policies, the more restrictive provisions will supersede.

3.2 IT Policy – 0501 – Use of IT Resources

3.3 IT Policy – 0502 – Virus Protection, Detection, and Removal

3.4 IT Policy - 0515 – Acceptable Uses for Portable Computers and Mobile Devices

3.5 IT Policy – 0519 – Data Transmission Security and Integrity

3.6 IT Policy - 0520 – Acceptable Workstation Use

3.7 DHHR Health Insurance Portability and Accountability Act (HIPAA) Policy 0441 – Safeguards to Protect the Privacy of Protected Health Information

3.8 DHHR HIPAA Policy 0449 – General Guidelines to Safeguard Protected Health Information.

3.9 OMIS OP-17 – Media Controls

3.10 OMIS OP-19 – Security for DHHR Portable Computers and Mobile Devices

3.11 OMIS OP-28 – Jump Drive Installation Instructions

4.0 RESPONSIBILITIES/REQUIREMENTS

4.1 To maintain protection against virus infections, employees **must** use OMIS-approved jump drives. Employee purchased jump drives, or those containing personal information, must **not** be connected to DHHR equipment at any time.

4.2 OMIS will evaluate, authorize, install, and maintain all software and hardware for use on all DHHR desktop computers, laptops, servers, and other computing devices.

4.3 Jump drives must contain OMIS-approved password and encryption software.

4.4 Employees are prohibited from using any DHHR system to store or transmit sensitive data or e-PHI that does not have adequate authorization mechanisms.

4.5 Employees should not store DHHR business related data on jump drives.

4.5.1 For security and convenience purposes, all DHHR business related data must be stored on the user's y: drive.

4.5.2 If a DHHR network connection is unavailable (ex: training outside of DHHR), jump drives may be used for short term data storage and back-up purposes only if approved by OMIS.

4.6 Transactions resulting from computer usage are the property of the DHHR, and are subject to DHHR policies as well as all applicable state and federal laws and statutes.

4.7 Bureaus/Offices may revoke the access rights of any individual at any time in order to protect data or to preserve the functionality of electronic information systems.

4.8 Enforcement Authority

4.8.1 The ISO is the person designated by the Chief Technology Officer (CTO) to monitor and provide initial enforcement of the DHHR's information security program and IT policies.

4.8.2 The Information Security Liaisons (ISL) are employees assigned by the Bureau Commissioners and/or Office Directors to assist the ISO in the protection of information resources.

4.8.3 The Office of the Inspector General (OIG) is the authority who investigates reported instances of Departmental employee misconduct.

4.9 Violations and Disciplinary Action(s)

4.9.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.

4.9.2 The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to his/her Office Director or Bureau Commissioner for appropriate action.

4.9.3 As determined by the Office Director or Bureau Commissioner, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.

4.9.4 Employees or systems administrators or managers who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to: (1) disciplinary action as outlined in DHHR Policy 2104; or (2) criminal prosecution.

5.0 DEFINITIONS

5.1 Equipment Coordinator (EC) – Designated employees in DHHR field offices, Child Care Resource and Referral agencies, and Local Health Departments who are responsible for providing first level computer support. ECs receive computer support direction from OMIS.

5.2 Jump Drive – A small self-powered drive that connects to a computer directly through a USB port.

5.3 Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.

5.4 USB Port – A device used for connecting peripherals (printer, scanner, modem, etc.) to a PC off of a single port.