POLICIES AND PROCEDURES
NEW JERSEY EARLY INTERVENTION SYSTEM

Date: May 1, 2011(Rev)

No.: **NJEIS-17**	Subject: **Computers & Electronic Records**
Effective Date: **May 1, 2011**	Category: **Information Technology**
Review Date: **April 2013**	Responsible Party: **Part C Coordinator**

I. Purpose

To protect personally identifiable information and minimize exposure to risks including virus attacks, compromise of networks systems and services, and legal issues when using computers.

II. Policy

A. NJEIS provider agencies must participate in the New Jersey Early Intervention System Management Information System (NJEIS-MIS), including the Central Management Office (CMO), purchase, inventory and/or use of standardized hardware and software required by the Department to implement the collection and reporting of uniform data.

B. NJEIS provider agencies must establish and enforce an acceptable computer use policy regardless of funding source and computer ownership.

1. Agency policy and procedures must meet or exceed the requirements established by the Department including record management and ensuring personally identifiable information is sanitized prior to the disposition of hardware and other storage devices.
2. All NJEIS provider agency personnel must sign a receipt acknowledging that they have received and read this and the agency's policy.

C. All computer hardware, software, and data provided by the early intervention system shall:

1. Only be used for NJEIS related activities;
2. Remain the property of the Department;
3. Be inventoried and reported to the Department or its assigned designee at least annually or upon request;
4. Cannot be disposed of or transferred without written permission from the Department; and
5. Be returned to the Department or its assigned designee upon contract termination (Grant/LOA) and/or the end of a designated purpose.

D. NJEIS provider agencies must maintain internet access and a current email address for each staff member to fully participate in the NJEIS-MIS.

E. Electronic transmissions of personally identifiable early intervention information from any computer must be encrypted or sent through a secure transmission.

F. Encryption must be used to protect early intervention data:
   1. "at rest" should physical security measures fail, such as files on computers and storage devices (e.g. USB flash drives).
   2. In transit (data being transferred via networks, mobile telephones, Bluetooth devices).

G. As used in NJEIS-17, the following words and terms are defined as indicated:
   1. **Encryption** is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable by unauthorized persons.
   2. **Electronic Record** means a record created, generated, sent, communicated, received, or stored by electronic means.
   3. **Record** is an item that documents a NJEIS transaction or action including but not limited to all correspondence, disks, maps, memoranda, papers, photographs, recordings, reports, tapes, writings and other data, information or documentary material, regardless of physical form or characteristics, storage media or condition of use made or received by an individual in connection with the provision of NJEIS services.
   4. **Record Management** means the planning, controlling, directing, organizing, training, promoting, and other managerial activities related to the creation, maintenance, use, and disposition of records.
   5. **Sanitized** for the purpose of protecting personally identifiable information means a procedure used to overwrite the hard drive.

H. Electronic communications must be conducted in a professional, responsible and courteous manner.

I. Antivirus software must be installed and regularly updated on computers used to conduct NJEIS business.

J. Under no circumstances are provider agency personnel to engage in any activity that is illegal under local, state, or federal law while utilizing NJEIS issued computers.

K. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use under the NJEIS while utilizing NJEIS issued computers will be subject to debarment from the NJEIS.

III. Procedures

A. **General Use and Ownership of Computer Hardware Provided by NJEIS**
   1. Authorized individuals from the assigned early intervention provider agency, the DHSS itself or an authorized NJEIS agent has the right to monitor/audit computers, systems and network traffic at any time**.**
   2. All computer hardware must:
      (a) retain the anti-virus software provided with the computer; and

(b) update the anti-virus software as recommended by the manufacturer

3. The use of agency specific encryption and/or anti-virus software for safeguarding data may be permissible if the agency provides acceptable justification and receives written approval from the Department.
4. No additional information including, but not limited to, an image, picture, icon, non-work related link, quote, phrase, or message shall be attached to electronic message**s.**
5. Email must include a confidentiality banner.
6. All NJEIS provider agency personnel must sign a receipt acknowledging that:
   (a) they have received and read this policy;
   (b) they will immediately report any breach of this policy to their supervisors;
   (c) the receipt of any property distributed by the Department for NJEIS related activities; and
   (d) the acknowledgement that the receipt must be kept on file at the provider agency's main administrative office**.**

B. **Security and Proprietary Information**

1. Agency personnel are responsible for ensuring that personally identifiable information residing on devices and electronic media, including storage media, will be removed before the devices and media are made available for internal reassignment in order to prevent unauthorized access to personally identifiable information.
2. NJEIS is responsible for ensuring that personally identifiable information residing on devices and electronic media, including storage media, will be removed before the devices and media are made available for external use (use by another agency) in order to prevent unauthorized access to personally identifiable information.
   (a) Disable the write caching and overwrite the hard drive with at least 33 passes of pseudo-random data.
   (b) If the hard drive includes bad sectors or it is not possible to overwrite with pseudo-random data then the hard drive must be destroyed through smelting or pulverizing.
   (c) Agency personnel using privately owned computers, devices and electronic media, including storage media are responsible for ensuring that personally identifiable information is protected and appropriately removed in order to prevent unauthorized access to personally identifiable NJEIS information.
3. Authorized provider agency personnel must:
   (a) Keep their passwords secure and not share account information.
   (b) Secure the computer with a password-protected screensaver by setting the automatic activation feature at 15 minutes or less, or by logging-off when left unattended.
   (c) Use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
4. Security breaches
   (a) NJEIS provider agencies must notify and document security breaches in writing to the lead agency immediately with the following information:
      - date of security breach;
      - type of security breach;

- a listing of the individuals affected by the security breach; and
- how and when the breach was corrected.

C. **Unacceptable Use of Computers Provided by NJEIS**

1. Authorized provider agency personnel are prohibited from:
   (a) Copying unauthorized copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the end user does not have an active license.
   (b) Installing any software on a NJEIS issued computer or altering its configuration unless undertaken by an administrator approved DHSS/NJEIS.
   (c) Engaging in instant messaging, playing Internet games, using streaming media or streaming video for non-NJEIS related purposes.
   (d) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.
   (e) Intentionally distributing malicious programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
   (f) Revealing account passwords to others or allowing use of an assigned account by others. This includes family and other household members.
   (g) Unauthorized transmission of confidential or proprietary information.
   (h) Using profane, harassing or other offensive language.
   (i) Using a NJEIS-issued computer to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
   (j) Making fraudulent offers of products, items, or services originating from any NJEIS-issued computer.
   (k) Effecting security breaches including, but not limited to, accessing data of which the individual is not an intended recipient or logging into a server or account that the individual is not expressly authorized to access, unless these duties are within the scope of regular duties.
   (l) Circumventing user authentication or security of any account.

2. **Internet Use Accessed through NJEIS Computer Hardware**
   (a) The sole purpose for which provider agency users may access the Internet using NJEIS-issued computers is to carry out NJEIS business.
   (b) Posting messages to large numbers of Usenet newsgroups (newsgroup spam), blogs, websites or any other Internet site utilizing any Internet protocol is prohibited.
   (c) NJEIS has the right to monitor Internet activity and therefore users should have no expectation of privacy.
   (d) All records created by Internet use, including path records, are the property of NJEIS and are subject to monitoring.
   (e) All users shall ensure that their use of the Internet does not compromise the security and integrity of the computer, whether by allowing intruders into the networks or by introducing viruses or other threats.

(f) In the event these polices do not address a specific concern or the user is unclear about the policy, they should consult their supervisor and/or the lead agency (DHSS).

D. **General Care and Security of Equipment Provided by NJEIS**

1. Provider agency users must take every precaution to safeguard the NJEIS-issued hardware from physical damage and /or a security breach of stored information.
2. Users must not eat or drink around the computer.
3. Computers must not be:
   (a) Left in the car as temperature can affect the unit and unattended computers in an automobile create an opportunity for theft;
   (b) Lent to other non-approved users; and
   (c) Personalized with pictures, notes, screensavers or decorations that would indicate the unit is personally owned.