Electronic Data and Computer Security Policy:

Electronic Security. These policies pertain to the security of confidential or “sensitive data” (defined below) and data stored or transmitted on university system computers, networks, or data storage devices -- including external hard drives, CDs, DVDs, disks, and “thumb drives”).

Sensitive Data:  
Refers to data that is held confidentially, and if compromised may cause harm to individual citizens or create a liability for the State or Montana University System. Examples include, but are not limited to:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:
  - Social security number;
  - Driver’s license number or state identification number;
  - Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

- Student transcripts, grades, and performance information;
- Health records or any information that would reveal medical history or the types of treatment an individual may have undergone;
- Insurance information;
- Criminal justice information;
- Trade secrets;
- Any HIPPA- or FERPA-regulated information.

OCHE Policies to Protect Electronic Data.

1. All employees must remove all confidential information from office personal computers, storage devices, or servers unless the data is critical to the performance of their respective jobs. The best defense against unauthorized data access is to not have the data in the first place.
2. No confidential information will be stored on OCHE personal computers, storage devices, or servers unless written permission has been granted by the IT Administrator and a security plan is developed and implemented. This plan will include, as a minimum, procedures to comply with the State of Montana’s Policy for Security of Sensitive Data (Appendix A).

3. Employees who need to archive or retain records containing confidential information must develop a document management plan for disposing of the information once it is no longer needed. This plan must be on record with the IT Administrator.

4. If confidential information needs to be retained or archived after initial use, this will not be done using any computer or storage device that is, or can be, connected to any network. Information should be transferred to removable storage medium (CD, DVD, etc.) or paper, removed from the computer, and the storage medium secured in a locked container.

5. No computer (including laptops) or storage device containing confidential information will be removed or transported from the OCHE office unless written permission has been granted through the IT Administrator and a security plan is developed and implemented. This plan will include, as a minimum, procedures to comply with the State of Montana’s Policy for Security of Sensitive Data (Appendix A).

6. Prior to removing or transport confidential information outside the OCHE office, a current copy of this data will be made and stored in a locked container within the OCHE office.

7. All individuals authorized to receive or maintain confidential information must maintain a current inventory and audit trail of what data is stored on which computers or storage devices. This inventory must be kept in enough detail so that if any computer or storage device is stolen, lost, or misplaced, whether within or outside the OCHE office, an accurate record is available to determine exactly what confidential information may have been compromised.

8. Confidential information will be stored or transported only on State-owned computers or storage devices.
9. No confidential information will be transported or stored on any computer or storage device transported outside the United States.

10. Computers or storage devices for which ownership is being transferred (disposed, donated to K-12, transferred to another MUS unit, etc.) will be cleaned of all confidential information and sanitized in accordance with BOR policy 1308 (Disposal of Computer Storage Devices).

11. All computers and storage devices must be turned off at the end of each business day, unless permission to do otherwise has been granted by the IT Administrator.

12. Laptops, external storage devices, and removable storage devices are especially vulnerable to theft. Unless otherwise secured by lock and cable, these items remaining in the office must be undocked/disconnected and stored in a locked compartment (file cabinet, locked desk drawer) at the end of each business day.

13. The following are prohibited on any computer owned by the state or operated on any MUS or State network:
   - Instant messaging of any type or form (Employees who have instant messaging software installed must contact the IT administrator to have it removed immediately);
   - Accessing any web site that requires a personal password to enter, unless that site is used exclusively for work related functions;
   - Opening any attachments on personal e-mail (pictures, video clips, electronic cards, documents, etc.).

14. Limited personal e-mail is unavoidable, but it should be kept to a bare minimum. Employees must remove themselves from any non-work related distribution lists.

15. Any individual who knows or suspects that confidential information has, or may have been, accessed by an unauthorized individual will immediately report the circumstances of the incident to the IT Administrator. Circumstances which must be reported include, but are not limited to, the following:
16. All employees must read and understand the State of Montana and Board of Regents policies regarding appropriate use of e-mail, Internet, and state-owned computers, printers, and other electronic devices. (The policies most relevant to individual employees are attached).

17. Enforcement actions for violations of this policy include, but are not limited to:

   o Disciplinary action for individuals, up to and including termination;
   o Denial of access to personal or sensitive data;
   o Revocation of network access privileges.

Other enforcement actions may be taken under MCA 2-17-514(1). In addition, individuals may be liable for costs incurred as a result of loss, theft, or unauthorized access of confidential information.
Employee Verification

I have read the OCHE Electronic Data and Computer Security Policy AND the Board of Regents policies 1302, 1303.1, 1303.2, and 1303.3. I understand and will comply with these policies.

(Employee Name – Print)

(Employee Name – Sign)     (Date)

__________
(Initial)  I do not possess or need to possess confidential information (as defined by State/Federal law) in the conduct of my work at OCHE.

__________
(Initial)  I need to receive or maintain confidential information in the conduct of my work at OCHE. (You will be contacted to establish a security plan for this data.)
Appendix A: Minimum Requirements for Use, Storage, or Transportation of Confidential Information.

The following minimum requirements apply to the use, storage, or transportation of confidential information by any employee. These requirements, and others as appropriate, will be included in the security plan approved by the IT Administrator before use, storage, or transportation of any confidential information is authorized.

Requirements:

Storage and Use of Confidential information is Restricted:

1. Departments and individuals shall collect, store, and use confidential information based solely on business requirements. These business requirements and the type of data collected, used, and stored must be documented.

2. Access shall be based on business requirements and limited solely to users authorized by management and the IT Administrator.

Confidential Information shall:

1. Not be copied or removed from secured storage environments unless there is a business requirement.

2. Not be used or stored outside of the OCHE office unless there is a business requirement approved by the department head and the IT Administrator.

3. Not be transmitted via non State-owned, or non-MUS owned, networks unless approved transmission protocols and encryption techniques are utilized.

4. Not be transported outside of the United States on any computer or storage device.

5. Only be stored on State-owned computers or storage devices if there is a business requirement.

6. Be encrypted when taken outside the OCHE office on any computer or storage device.
7. Not be transferred to non State-owned computers or storage devices unless approved by the IT Administrator.

8. Maintain a current audit trail and inventory of who has what confidential information, on what computer or device, and for what business purpose.

Device Configuration Procedures:

Users of computers or storage devices containing confidential information are required to configure and properly secure the device. Based on device capability:

1. Configure the device as required in State IT Policy ENT-SEC-112.
2. Configure the login banner to be enabled during travel, adding contact information and explicit instructions on how to return the portable device to the information required in State IT Policy ENT-SEC-112.
3. Disable file- and print-sharing functions.
4. Ensure there is a required logon for the operating system.
5. Disable Auto-Logon features.
6. Use passwords that conform to the requirements and guidelines of State IT Policy ENT-SEC-063.
7. Ensure there is a backup of data within a secured storage environment.

Physical Security Procedures:

Physical security procedures undertaken by users with computers or storage devices containing confidential information in their custody includes, as a minimum, the following:

1. Ensure the computer or device has an asset/property tag containing appropriate contact information.
2. Label all computers or devices for individual identification.
3. Do not leave computers or devices unattended in non-secured areas.
4. Do not leave computers or devices in an unlocked vehicle; place computers and devices in a locked trunk or out of plain sight in the locked passenger compartment.

5. Store computers or devices in a safe when staying in a hotel.

6. Monitor the whereabouts of the computer or device as they pass through airport security checkpoints and retrieve them as soon as possible to minimize the risk of loss or theft.

7. Confer with the IT Administrator for specific technology selections and implementation procedures for encryption of data.

Operational Procedures:

When accessing confidential information from a non-state network:

1. Use only secure web clients.

2. Do not transfer confidential information to another device not in compliance with this policy.