

Information Security Policy

May 21, 2008

Information Security Policy	3
Goal of the Information Security Policy	3
Purpose of Information Security Policy	3
Summary of Personal Responsibilities	4
General Principles	4
Accountability	4
Information Collections and the Responsibilities of Data Owners	4
Responsibilities of ODE Management Team	5
User Responsibilities	5
Protecting Information Wherever It Is Located	5
Diligence Concerning Information Associated with “Identity Theft”	6
Limitations on Sharing Personally Identifying Information	6
Methods of Distributing Public Information Associated with Individuals	7
Exchanging Information via E-Mail or Other Network Facilities	7
Discarding Information	8
Valid Uses of Aggregate Information	8
Subpoenas	8
Reporting of Security Breaches or Suspicious Activity	8
Awareness Prior to Obtaining Access to Confidential Information	9
Additional Requirements for Technology Managers	9
Appendix A - Personally Identifying Information That Is Generally Considered Public	10
Information about Current and Former Students	10
Information about Parents, Guardians and Sponsors	10
Information about Faculty and Staff	11
Appendix B -Potentially Applicable Laws	12
Computer Fraud and Abuse Act (CFAA)	12
Electronic Communications Privacy Act (ECPA)	12
The Family Educational Rights and Privacy Act (FERPA)	12
Health Insurance Portability and Accountability Act (HIPAA)	13
The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act (GLBA))	13
The Technology, Education, and Copyright Harmonization Act (TEACH Act)	13
State Laws	13
Subpoenas and Other Compulsory Requests	14
Vendor Agreements	14
Appendix C – Table of Data Owners and Designated Contacts	15
Table of Data Owners and Designated Contacts	16
Table of Data Owners and Designated Contacts (continued)	17
Appendix D – How Data Owners Assess Security Requirements	18
Appendix E – Summary of End User Responsibilities	20
Protection of Confidential Information – Summary of Responsibilities	21
Appendix F – Enterprise Security Office Policies	22

Information Security Policy

Goal of the Information Security Policy

The goal of the Information Security Policy is to ensure that the...

- Confidentiality,
- Integrity and
- Availability

Of each piece of information owned by or entrusted to Oregon Department of Education (ODE) is protected in a manner that is consistent with...

- The value attributed to it,
- The risk that ODE is willing to accept and
- The cost that ODE is willing to pay (in dollars and convenience)

Wherever it resides, i.e.:

- On printed media (e.g., forms, reports, microfilm, microfiche, books),
- On computers,
- On networks,
- On magnetic or optical storage media (e.g., hard drive, diskette, tape, CD),
- In physical storage environments (e.g., offices, filing cabinets, drawers),
- In a person's memory, etc.

Purpose of Information Security Policy

The purpose of this document is to define the principles to which all ODE staff must adhere when handling information owned by or entrusted to ODE in any form. The principles cover the following areas:

- Defining the confidentiality, integrity and availability requirements for information used to support ODE's objectives,
- Ensuring that those requirements are effectively communicated to individuals who come in contact with such information, and
- Using, managing and distributing such information – in any form, electronic or physical -in a manner that is consistent with those requirements.

This policy describes in general terms the Information Security Policy of ODE, which is also embodied in various policies developed by the guardians of specific information.

Summary of Personal Responsibilities

While much of this policy document focuses on our legal obligations and the process of determining and communicating the sensitivity of information owned by or entrusted to ODE, it also contains a number of requirements to which anyone who handles such information must adhere. In summary:

- You are responsible for your use or misuse of confidential information.
- You must not in any way divulge, copy, release, sell, loan, review, alter or destroy any information except as properly authorized within the scope of your professional activities.
- You must take appropriate measures to protect confidential information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.
- You must safeguard any physical key, ID card or computer/network account that allows you to access confidential information. This includes creating computer passwords that are difficult to guess.
- You must render unusable confidential information held on any physical document or computer storage medium (e.g., diskette, CD, magnetic tape, hard disk) that is being discarded.
- You must report any activities that you suspect may compromise confidential information to your immediate supervisor or to the ODE Information Security Officer (ISO), or Chief Information Officer (CIO).

General Principles

Accountability

All information gathered and maintained by employees of ODE for the purpose of conducting business is considered institutional information and, as such, each individual who uses, stores, processes, transfers, administers and/or maintains this information is responsible and held accountable for its appropriate use.

Information Collections and the Responsibilities of Data Owners

Information that is held by ODE must be protected against unauthorized exposure, tampering, loss and destruction, wherever it is found, in a manner that is consistent with applicable federal and state laws (see Appendix B), and with the information's significance to ODE and any individual whose information is collected. Achieving this objective requires that ODE information be segregated into logical collections (e.g., medical records, employee benefit data, payroll data, student records, financial records), and that each collection be associated with an individual known as a "Data Owner" who must:

- Define the collection's requirements for confidentiality, integrity and availability (see Appendix D for requirement classifications),
- Convey the collection's requirements in writing to the managers of departments that will have access to the collection,

- Work with the ODE management team to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information).

The Data Owner of a logical information collection is typically the head of the department on whose behalf the information is collected or that is most closely associated with such information. A list of Data Owners and their designated contacts may be found in Appendix C.

Each Data Owner may designate one or more individuals on his or her staff to perform the above duties. However, the Data Owner retains ultimate responsibility for their actions.

Responsibilities of ODE Management Team

ODE management team is required to:

- Understand the security-related requirements for the information collections used within their respective departments by working with the appropriate Data Owners, and their designated staff.
- Develop procedures that support the objectives for confidentiality, integrity, and availability defined by the Data Owners and designated staff, and ensure that those procedures are followed.
- Effectively communicate any restrictions to those who use, administer, process, store or transfer the information in any form, physical or electronic.
- Ensure that each staff member understands his or her information security-related responsibilities and acknowledges that he or she understands and intends to comply with those requirements by having them review the “Protection of Confidential Information – Summary of Responsibilities” document contained in Appendix E.
- Report any evidence that information has been compromised or any suspicious activity that could potentially expose, corrupt or destroy information to the ODE ISO.

User Responsibilities

Protecting Information Wherever It Is Located

Each individual who has access to information owned by or entrusted to ODE is expected to know and understand its security requirements and to take measures to protect the information in a manner that is consistent with the requirements defined by its Data Owner, wherever the information is located, i.e.,

- On printed media (e.g., forms, reports, microfilm, microfiche, books),
- On computers,
- On networks (data and voice),
- On magnetic or optical storage media (e.g., hard drive, diskette, tape, CD),
- In physical storage environments (e.g., offices, filing cabinets, drawers),
- In a person’s memory, etc.

If an authorized user is not aware of the security requirements for information to which he or she has access, he or she must provide that information with maximum protection until its requirements can be ascertained.

Any individual who has been given a physical key, ID card or logical identifier (e.g., computer or network account) that enables him or her to access information is responsible for all activities performed by anyone using that key or identifier. Therefore, each individual must be diligent in protecting his or her physical keys and ID cards against theft, and his or her computer and network accounts against unauthorized use. Passwords created for computer and network

accounts should be difficult to guess (see “Password Policy” document for guidelines). Furthermore, passwords should never be shared or recorded and stored in a location that is easily accessible by others. Stolen keys and ID cards, and computer and network accounts suspected of being compromised should be reported to the appropriate authorities immediately.

The assignment of a single network or system account to a group of individuals sharing the same password is highly discouraged and may only occur in cases where there is no reasonable, technical alternative.

Diligence Concerning Information Associated with “Identity Theft”

Identity theft is a serious and growing problem in our society. Anyone who can obtain certain pieces of information about an individual can open credit cards, take out loans, create forged documents or steal assets in the individual’s name.

Being sensitive to the identity theft threat, ODE requires that extra precaution be taken when collecting, using and storing non-public “personally identifiable” information, such as:

- Social Security Number,
- Date of birth,
- Place of birth,
- Mother’s maiden name,
- Credit card numbers,
- Bank account numbers,
- Income tax records, and
- Drivers license numbers.

Collection and use of any of the above pieces of information should be limited to situations where there is legitimate business need and no reasonable alternative. Managers must ensure that their employees understand the need to safeguard this information, and that adequate procedures are in place to minimize this risk. Access to such information may only be granted to authorized individuals on a need to know basis.

Limitations on Sharing Personally Identifying Information

All non-public information gathered and maintained by employees of the Oregon Department of Education, for the purpose of conducting business, that personally identifies any living or deceased individual – names and other personal information pertaining to individual students, faculty, staff, alumni, parents, guardians, spouses, children, donors, beneficiaries, etc. – is considered “confidential” unless otherwise specified by this document or by the appropriate Data Owner or designate. Such information associated with an individual may only be shared with:

- The individual with respect to whom the information is maintained,
- Persons designated in writing by that individual,
- ODE employees and representatives (included selected volunteers) who need access to such information for legitimate ODE business or to support the processing of such information, and who are authorized by the appropriate Data Owner or designate,
- Governmental agencies to which ODE has a legal obligation to provide such information,
- ODE-contracted organizations that:
 - Require such information to deliver their services on behalf of ODE,

- Are authorized by the appropriate Data Owner, and
- Are bound by appropriate, non-disclosure agreements. An organization receiving non-public financial information must execute a Confidential Information Addendum (See Appendix F).

The use of any personally identifying information collected and/or maintained by ODE about any living or deceased individual – students, faculty, staff, alumni, parents, guardians, spouses, children, donors, beneficiaries, etc. – in hard copy or electronic form for any purpose that does not support ODE’s objectives (e.g., political or commercial solicitations), is strictly prohibited.

Methods of Distributing Public Information Associated with Individuals

Some pieces of personally identifiable information are considered public information. These pieces of information are described in Appendix A. The following procedures describe how public information associated with individuals may be shared:

- Directory information, including name, office address and phone number (ODE staff) and e-mail address, can be made generally available over the electronic ODE web site. The appropriate Data Owner may deem other elements of information as directory information as well.
- Other public information may be released in response to reasonable requests.

Exchanging Information via E-Mail or Other Network Facilities

Electronic mail (e-mail) may in most situations be considered an insecure mechanism for exchanging information. The privacy of information contained within e-mail messages can be exposed, especially when either the sender or any of the recipients are not on the ODE network, or utilize a wireless network connection. The use of mechanisms that exchange information in a readable form, such as “ftp”, “chat” and “instant messaging”, between on-and off-campus computers also places confidential information at risk.

If information, deemed by its Data Owner as “confidential” or “highly confidential”, must be exchanged with an individual or entity outside of the ODE using e-mail or any other network facility that transfers data, it must be encrypted using a hardware-or software-based mechanism approved by the Office of Assessment and Information Systems.

All business-related e-mail containing “confidential” or “highly confidential” information sent to recipients who are not in the “ode.state.or.us” domain must include the following disclaimer:

“This electronic communication, including any attached documents, may contain confidential and/or legally privileged information that is intended only for use by the recipient(s) named above. If you have received this communication in error, please notify the sender immediately and delete the communication and any attachments.”

Discarding Information

Physical documents containing information that has been classified as “confidential” or “highly confidential” by their Data Owners and/or designates must be shredded using an ODE approved device or shredding facility prior to being discarded.

Any computer hard drive or removable magnetic medium, such as a diskette, magnetic tape, Zip disk, etc., that has been used to hold any kind of “confidential” or “highly confidential” information must be electronically “scrubbed” to Department of Defense 5220.22-M standards using OASIS approved software prior to being discarded or being transferred to any individual or entity who is not authorized to view such information. On such media, the mere deletion of confidential data is not sufficient as deleted information is still accessible to individuals possessing any of a number of available software tools. Any non-erasable medium, such as a CD, optical disk, etc., that has been used to hold any kind of “confidential” or “highly confidential” information must be physically destroyed before being discarded.

Valid Uses of Aggregate Information

Authorized users may analyze and aggregate institutional data. However, official, published reports that include such aggregate data may only be issued with the review and approval of the appropriate Data Owner. Similarly, sharing those reports with individuals or organizations for which the reports are not primarily intended requires the permission of the individual or office primarily responsible for the report.

Subpoenas

Authorized users are reminded that the full range of information collected on any living or deceased individual – students, faculty, staff, alumni, parents, guardians, spouses, children, donors, beneficiaries, etc. – in hard copy or electronic form may be subpoenaed and entered into the public record of a court case. Appropriate discretion should therefore be exercised in the drafting of any document that will be stored in any ODE file.

Employees who receive investigative subpoenas, court orders and other compulsory requests from law enforcement agencies that require the disclosure of ODE held information should contact the ODE management team before taking any action.

Reporting of Security Breaches or Suspicious Activity

Any member of ODE staff who comes across any evidence of information being compromised or who detects any suspicious activity that could potentially expose, corrupt or destroy information must report such information to his or her immediate supervisor or to the ODE ISO, or the ODE CIO. No one should take it upon himself or herself to investigate the matter further without the authorization of the ODE Security Officer or CIO.

Awareness Prior to Obtaining Access to Confidential Information

All individuals must review the “Protection of Confidential Information – Summary of Responsibilities” document contained in Appendix E before being given access to confidential information contained within ODE’s computer systems, networks and physical facilities.

Additional Requirements for Technology Managers

Technology managers are those individuals who manage computing and network environments where ODE information is stored, transmitted or processed, such as:

- Computer operating environments (e.g., Windows, Macintosh, etc.),
- Database management environments (e.g., SQL Server, Access, etc.),
- Application environments (e.g., Exchange, web applications, etc.),
- Network environments (e.g., electrical, optical, and wireless networks, routers, switches, firewalls, etc.),
- Physical storage facilities (e.g., tape libraries, filing cabinets, etc.),

Technology managers are responsible for ensuring that specific data’s requirements for confidentiality, integrity and availability as defined by the appropriate Data Owner are being satisfied within their environments. This includes the development of:

- A cohesive architectural policy,
- Product implementation and configuration standards,
- Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Data Owners, and
- An effective strategy for protecting information against generic threats posed by computer hackers.

Appendix A - Personally Identifying Information That Is Generally Considered Public

Notwithstanding the general policy of treating personally identifying information as “confidential”, the information listed below describes the circumstances under which certain limited types of personally identifying information may be generally considered by ODE to be publicly accessible, except as otherwise noted. Other elements may only be considered public if defined as such by the appropriate Data Owner.

Information about Current and Former Students

While the Family Educational Rights and Privacy Act (FERPA) generally prohibits the public disclosure of information regarding current and former students that was collected during their enrollment (see Appendix B -Potentially Applicable Laws), FERPA does allow for the public disclosure of certain “Directory Information” that may be shared with the general public, provided that the given student has not expressly objected to such disclosure.

ODE considers the following to be “Directory Information” that may be shared with the general public:

- Name,
- Local address,
- Local telephone number,
- E-mail address,
- Photo,
- Dates of attendance,
- Major field of study,
- Participation in officially recognized activities, organizations and athletic teams,
- Weight and height of members of athletic teams,
- Degrees and awards,

There are additional data elements, identified within FERPA as being available for public disclosure, which ODE has decided to keep confidential or internal as a matter of policy. The following elements must be treated as “confidential”:

- Date of birth,
- Place of birth.

The following must be treated as “internal”:

- Home address,
- Home telephone number.

Information about Parents, Guardians and Sponsors

The following information about parents, guardians and sponsors is considered to be public:

- Name,
- Address (home and local),
- Relationship to student.

Information about Faculty and Staff

The following information about current and former staff and faculty is considered to be public:

- Name,
- Dates of his or her affiliation with the institution,
- Office address and phone number,
- E-mail address,
- Title and/or job function.

DRAFT

Appendix B -Potentially Applicable Laws

As summarized below, a number of federal and state laws may also apply to information collected and maintained by ODE employees. Please direct questions regarding the applicability of these laws and other potential legal issues to the Office of General Counsel.

Computer Fraud and Abuse Act (CFAA)

Enacted in 1984 (and revised in 1994), the CFAA criminalizes unauthorized access to a “protected computer” with the intent to defraud, obtain any information of value or cause damage to the computer. Under the CFAA, a “protected computer” is defined as a computer that is used in interstate or foreign commerce or communication or that is used by or for a financial institution or the government of the United States. For example, the act of “hacking” into a secure web site from an out-of-state computer may violate the CFAA.

Electronic Communications Privacy Act (ECPA)

Enacted in 1986, the ECPA broadly prohibits (and makes criminal) the unauthorized use or interception of the contents or substance of wire, oral or electronic communications. In addition, the ECPA prohibits unauthorized access to or disclosure of electronically stored communications or information. Such prohibitions may apply to ODE employees who willfully exceed the scope of their duties or authorizations by accessing certain databases housed within the ODE system. The ECPA does not, however, prohibit ODE from monitoring network usage levels and patterns in order to ensure the proper functioning of its information systems.

The Family Educational Rights and Privacy Act (FERPA)

Enacted in 1974, FERPA (also known as the Buckley Amendment) affords students (or parents if the student is a minor) certain rights with respect to the student’s “education records.” As defined under FERPA, the term “education records” encompasses a broad range of materials and information such as disciplinary, financial and academic records established during a given student’s enrollment and maintained in a variety of ODE databases and other filing arrangements. In particular, FERPA provides that “education records” and personally identifiable information contained therein may not be released or disclosed (including disclosure by word of mouth) without the written consent of the student (or parents, as the case may be). Violations of FERPA may result not only from the unauthorized disclosure of education records but also from the failure to exercise due care in protecting such records against unauthorized access from outsiders. However, even in the absence of express student (or parental) consent, FERPA permits disclosure of education records to ODE employees who have a legitimate interest in the student and to outside parties in a variety of circumstances, such as those where public health or safety are at issue.

Health Insurance Portability and Accountability Act (HIPAA)

Enacted in 1996, HIPAA sets national privacy standards for the protection of certain types of health information to the extent such information is electronically transmitted by health plans, health care clearinghouses, and health care providers. ODE is subject to HIPAA as a provider of employee group health plans. Accordingly, with respect to such health plans, ODE has (a) adopted written privacy procedures describing who has access to protected health information, how such information will be used, and when it may be disclosed; (b) required business associates to protect the privacy of such health information; (c) trained employees in the applicable privacy policies and procedures; and (d) designated a Privacy Officer to be responsible for ensuring that such policies and procedures are followed. HIPAA may also apply to certain research activities such as the collection and use of personally identifying health information from patient populations in clinical settings.

The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act (GLBA))

Enacted in 1999, the GLBA requires financial institutions to carefully protect customers' financial information. Universities are "financial institutions" by virtue of their loan servicing and therefore must comply with GLBA provisions. The GLBA has two relevant components: (1) "safeguarding" rules and (2) privacy rules. All personally identifiable financial information from students, parents, and employees must be safeguarded against foreseeable risks of disclosure, intrusion and systems failure. ODE has designated information security program managers in the business units that handle financial information, identified risks to the security of financial information, and is developing security programs to protect against risks. As the privacy standards of GLBA must be followed for all non-student financial information, ODE is developing a privacy policy to comply with GLBA and will make required privacy notifications to non-student customers whose financial information is obtained. More information is available on the Federal Trade Commission web site:

<http://www.ftc.gov/privacy/glbaact/index.html>

The Technology, Education, and Copyright Harmonization Act (TEACH Act)

Enacted in 2002, the TEACH Act relaxes certain copyright restrictions so that accredited, non-profit colleges and universities may use multimedia content for instructional purposes in technology-mediated settings. However, the TEACH Act carries a number of security requirements designed to ensure that digitally transmitted content will be accessible only to students who are properly enrolled in a given course.

State Laws

In addition to the federal laws summarized above, there may be particular state laws that apply to the handling of confidential information. For example, state laws may govern the collection or use of information regarding children, consumers and other groups.

Subpoenas and Other Compulsory Requests

Many of the federal and state laws described above create exceptions allowing for the disclosure of confidential information in order to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies. Employees who receive such compulsory requests should contact the Office of General Counsel before taking any action.

Vendor Agreements

When negotiating contracts with third party vendors, ODE employees should consider whether such vendors require access to ODE databases or to other filing systems containing confidential information. Agreements providing third party vendors with access to such information must ensure that the vendor is subject to obligations of confidentiality that will enable the ODE to comply with its own obligations under the applicable privacy laws. In addition, such vendors should be contractually obligated to implement data protection and security measures that are commensurate with the ODE's practices. By the same token, ODE employees must be careful not to disclose confidential information entrusted to their care by an outside party, especially when such information is governed by the terms of a confidentiality agreement or clause with that party.

DRAFT

Appendix C – Table of Data Owners and Designated Contacts

As previously stated within this document, the guardian of a logical collection of information is typically the head of the department on whose behalf the information is collected or who is most closely associated with such information. For each assigned information collection, each Data Owner or individual whom he or she designates is required to:

- Define the collection's requirements for confidentiality, integrity and availability (see Appendix D for requirement classifications),
- Convey the collection's requirements in writing to the managers of departments that will have access to the collection.
- Work with ODE management team to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information),

Authorized users are required to understand the security-related requirements associated with the information with which they come into contact.

The table on following page lists information collections, their guardians and designated contacts:

DRAFT

Table of Data Owners and Designated Contacts

Information Collections Pertaining to...	Information Guardian	Designated Contacts
<p><u>Students:</u></p> <p>The physical or mental health of any student.</p>		
<p><u>Faculty and Staff:</u></p> <p>Work related injuries for active employees or those on long and short term disability.</p>		
Applicants – Employees and related staff		
Applicants – Staff		
Current Faculty and their related staff		
Staff		
Dependents and beneficiaries of Faculty and Staff		
<p><u>Alumni and Donors:</u></p> <p>Alumni (Personal Information)</p>		
Donors		

Table of Data Owners and Designated Contacts (continued)

Information Collections Pertaining to...	Information Guardian	Designated Contacts
<u>ODE Operations:</u> Academic/Administrative Departments		
Community Affairs		
Facilities		
Financial Matters		
Law Enforcement and Public Safety		
Legal Matters	General Counsel	
Library Records		

DRAFT

Appendix D – How Data Owners Assess Security Requirements

As stated previously, Data Owners are responsible for assessing the security requirements for each of their assigned information collections across three areas of concern: confidentiality, integrity and availability. To facilitate the assessment process and ensure that these requirements are expressed in a consistent manner across the ODE, Data Owners and designates will be required to categorize their information collections using the guidelines described in this section.

The **confidentiality** requirement for an all data will be expressed in the following terms:

- **Level 1 Published** - Low sensitive information that will not jeopardize the privacy or security of agency employees, clients and partners. *Examples: Press releases, brochures, pamphlets, etc.*
- **Level 2 Limited** - Sensitive information that may jeopardize the privacy or security of agency employees, clients, partners. *Examples: internal audit reports, names and addresses not protected from disclosure, enterprise risk management planning documents.*
- **Level 3 Restricted** - Sensitive information, unauthorized access could result in financial loss or identity theft. *Examples: Network diagrams, personally identifiable information, other information exempt from public records disclosure.*
- **Level 4 Critical** - Extremely sensitive, potential to cause major damage or injury. *Examples: Disclosure that could result in the loss of life, disability or serious injury or regulated information with significant penalties for unauthorized disclosure, information that is generally exempt from public disclosure.*

The **integrity/availability** requirement for an information collection will be expressed as follows:

- **“Non-critical”** if its unauthorized modification, loss or destruction would cause little more than temporary inconvenience to the user community and support staff, and incur limited recovery costs. Reasonable measures to protect information deemed “non-critical” include storing physical information in locked cabinets and/or office space, using standard access control mechanisms that prevent unauthorized individuals from updating computer-based information, and making regular backup copies.
- **“Critical”** if its unauthorized modification, loss, or destruction through malicious activity, accident or irresponsible management could potentially cause ODE to:
 - Suffer significant financial loss or damage to its reputation,
 - Be out of compliance with legislative requirements,
 - Adversely impact its clients, or
 - Miss a legally mandated deadline.

In addition to the protective measures described for information deemed “non-critical”:

- “Critical” information must be verified either visually or against other sources on a regular basis, and
- A business continuity plan to recover “critical” information that has been lost or damaged must be developed, documented, deployed and tested annually.

DRAFT

Appendix E – Summary of End User Responsibilities

All individuals must review the following “Summary of Responsibilities” document before obtaining access to confidential information contained within ODE computer systems, networks and physical facilities.

ODE management team are responsible for ensuring that each of their staff members who have access to confidential information has reviewed the document and understands his or her responsibilities as they relate to the handling of confidential information.

DRAFT

Protection of Confidential Information – Summary of Responsibilities

Applicable to: All Individuals with Access to Confidential ODE Information

Effective Date: May 21, 2004

ODE maintains information that is sensitive and valuable, and is often protected by Federal and State laws that prohibit its unauthorized use or disclosure. This includes, but is not limited to:

- Personal information about faculty, staff, students, parents, alumni or donors (e.g., social security numbers, dates and places of birth, mother's maiden names, student records, employment records, disciplinary actions, credit card numbers, financial data, medical records, etc.)
- ODE business information (e.g., financial reports, internal reports and memos, contracts, strategic reports, surveys, etc.)
- Information about or provided by third parties (e.g., information covered by non-disclosure agreements, contracts, business plans, non-public financial data, computer programs, etc.)

The exposure of such information to unauthorized individuals could cause irreparable harm to ODE. Thus, you are expected to diligently protect it:

- You may only access the information needed to perform your legitimate duties as an ODE employee and only after being authorized by the appropriate Data Owner.
- You may not in any way divulge copy, release, sell, loan, review, alter or destroy any information except as properly authorized within the scope of your professional activities.
- You must take appropriate measures to protect confidential information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.
- You must safeguard any physical key, ID card or computer/network account that allows you to access confidential information. This includes creating difficult-to-guess computer passwords.
- You must destroy or render unusable confidential information held on any physical document (e.g., memos, reports, microfilm, microfiche) or computer storage medium (e.g., diskette, CD, magnetic tape, hard disk) that is being discarded.
- You must report any activities that you suspect may compromise confidential information to your immediate supervisor or to the ODE Information Security Officer.
- Your obligation to protect confidential information does not cease after you leave ODE.

Your failure to comply with the above requirements may subject you to disciplinary measures, up to and including termination of employment.

Appendix F – Enterprise Security Office Policies

The following policies were all developed by the State of Oregon Enterprise Security Office (ESO). If you would like to know more about these policies go to the referencing URL located with each policy. If you would like to know more about the ESO and their mission, please go to their website located at <http://oregon.gov/DAS/EISPD/ESO/index.shtml>.

Incident Response Policy, Number: 000-000-000, Effective Date: 00-00-00

Transporting Information Assets, Number: 107-004-100, Effective Date: 01-31-08,
http://oregon.gov/DAS/OP/docs/policy/state/107-004-100_013108.pdf

Information Asset Classification, Number: 107-004-050, Effective Date: 01-31-08,
http://oregon.gov/DAS/OP/docs/policy/state/107-004-050_013108.pdf

Employee Security, Number: 107-004-053, Effective Date: 07-30-07,
<http://oregon.gov/DAS/OP/docs/policy/state/107-004-053.pdf>

DRAFT