Oklahoma State University Policy and Procedures

ELECTRONIC USE OF SOCIAL SECURITY NUMBERS	**3-0322** **ADMINISTRATION & FINANCE** **Information Technology** **July 2008**

PURPOSE AND SCOPE

1.01 The OSU/A&M System is committed to maintaining the confidentiality of sensitive and personal information. This policy applies to all individuals and University units that collect, use, store and transmit Social Security Numbers (SSNs).

OBJECTIVES

2.01 In issuing this policy, the University is guided by the following objectives.

A. Increase awareness of the confidential nature of SSNs and the risk of identity theft related to unauthorized disclosure and reduce collection of SSNs except where authorized by law or approved administrative exceptions.

1. Laws governing the authorized use and storage of SSNs are listed in section 5 of this policy.

2. Exceptions for the use and storage of SSNs are listed in section 6 of this policy.

B. Reduce the use of SSNs in records and information systems, including display screen and printed reports and reduce electronic storage of SSNs to a minimum number of locations with the goal being one location.

C. Create consistent policies regarding the collection, storage, use and disclosure of SSNs throughout the University and increase the confidence of students, employees and affiliates/guests that their SSNs are handled in a confidential manner.

POLICY

3.01 The Information Technology (IT) Information Security Office has the oversight responsibility for the use of SSNs.

3.02 Every OSU department and/or unit, including branch campuses, that collect, store, or transmit SSNs must report that use to the IT Information Security Office. A centralized inventory will be maintained for all approvals and exception requests. Systems that collect or

store social security numbers, which have not been approved by the IT Information Security Office, will be in violation of this policy.

3.03 All electronic systems requiring a unique OSU/A&M system wide identifier for faculty, staff and students must use the campus-wide identifier (CWID) as assigned by the enterprise administrative system. Therefore, the collection and use of SSNs will be limited to what is authorized by law or administrative exception. No one should ever access a data file that contains SSNs without a legitimate business purpose.

3.04 Any system using SSNs requires authentication for system access, masking or encryption for transmission, and encryption for storage. Temporary exceptions may be granted only if the data owner adheres to alternative security measures. Zip files will suffice for the encryption but they must be password protected.

3.05 New purchases or development of software systems that necessitate the use of SSNs will require prior approval from the IT Information Security Office.

3.06 SSNs should never be stored on auxiliary storage devices such as thumb drives and CDs or sent in plain text via email.

3.07 All security breaches and inappropriate disclosers of SSNs will be reported to the IT Information Security Office.

PROCEDURE

4.01 Approval: All approval requests for new and/or continued use of SSN's must be entered into the "AIRS" (Administrative Information Resource System) located at http://airs.okstate.edu/ and then reviewed by the IT Information Security Office.

4.02 Conversion: Systems currently using SSNs as primary identifiers that do not fall under the exemption section must convert to CWID. Those needing a cross reference file to perform the conversion will submit a help ticket to helpdesk@okstate.edu. Do not send any data at this time. You will receive further instructions on how to transmit the file by IT personnel.

4.03 Annual review: The IT Information Security Office will conduct an annual review of all production systems authorized to use SSNs.

4.04 Access & Transmission

A. If you access the network remotely, a virtual private network (VPN) is required. The client for the OSU/A&M VPN solution can be downloaded at the IT Software Distribution Website.

B. SSNs are not to be transmitted over the network/Internet unless they are encrypted or the connection is secure.

C. Departments that fall in the exception category must ensure that the SSNs are encrypted and only stored on OSU-owned computers/servers.

D. Mobile devices, laptop computers, PDAs, etc, that house SSNs must employ a whole disk encryption solution, such as that offered by the IT Information Security Office.

4.05 Responsibilities: All employees are tasked with keeping sensitive and personal information confidential.

A. All departments will be required to annually verify their usage of SSNs. This includes hard drives on servers, desktop computers and laptops as well as group and home drives. Software to perform this check can be found on the IT Software Distribution Website. Vice Presidents and Deans will be contacted by the IT Information Security Office when their review is to be conducted.

B. If your job requires you to view and/or update SSNs, ensure that the public and other unauthorized individuals cannot view your monitor. Secure your workstation from unauthorized use by locking your workstation when you step away from your desk and log off or shut down your workstation when you leave the office for the day. Properly dispose of any written SSNs by shredding the document.

4.06 The Office of Financial Information Management will maintain the Administrative Information Resource System.

4.07 Please contact your local IT support personnel or the IT Help Desk for assistance with any of the preceding security measures.

RELATED LAWS, REGULATIONS AND POLICIES

5.01 Federal: Privacy Act of 1974; Family Education Rights and Privacy Act (FERPA); Gramm-Leach-Bliley Act (GLB-A); and the Health Insurance Portability and Accountability Act (HIPAA).

5.02 State: Oklahoma law: Title 74, Chapter 49, Section 3113.1, "Disclosure of Security Breach of Personal Computer Data - Notice to Owner or Licensee of Personal Data – Exception"; Oklahoma law: Title 74, Chapter 49, Section 3111, "Use Of Social Security Numbers By State Or Subdivisions Prohibited – Exceptions"; Oklahoma law: Title 40, Chapter 5, Section 173.1, "Employees' Social Security Numbers"; and Oklahoma law: Title 85, Chapter 2, Section 26, "Workers Compensation."

EXCEPTIONS

6.01 While the collection and use of SSNs may be required for certain legal and business activities, approved use does not include retention of this information by departments without specific approval as required within this policy. Approved uses of the SSN by the University, which may be limited to specific departments, are listed below.

A. University Admissions Process: Information systems used by the University admissions process will be permitted to use SSNs.

B. Employment: SSNs are required for a variety of employment matters; such as proof of citizenship, tax withholding, FICA, or Medicare.

C. Application and Receipt of Financial Aid: Students applying for student aid using the Federal Free Application for Student Assistance (FAFSA) are required to provide SSNs. Students must also provide SSNs when applying for student education loans.

D. Tuition Remission: SSNs are required for state reporting of taxable tuition remission benefits received by employees, their spouses and dependents, and by graduate assistants.

E. Accounts Receivable Management: The University maintains contractual agreements with accounts receivable management entities. These entities require SSNs to perform their activities for the University.

F. Benefits Administration: SSNs are often required for verifying enrollment, processing and reporting on various benefit programs, such as medical benefits, health insurance claims and veterans' programs.

G. IRS Reporting: SSNs are used for federally required reporting to the IRS. For example, the University reports the value of all taxable and non-taxable scholarships and grants awarded to non-resident aliens to the IRS.

H. Student Information Exchange: SSNs may be used for the exchange of information from student academic records between appropriate institutions, including other colleges and universities or certification and licensure programs.

I. The IT Information Security Office is authorized to possess SSNs for law enforcement requests, internal investigations and security breaches.