CALIFORNIA STATE UNIVERSITY, NORTHRIDGE
UNIVERSITY STUDENT UNION, INC.

CORPORATE POLICY

SUBJECT: **Fusion Technology and CSUN Data Downloads**

REFERENCE: Information Practices Act (IPA) California Civil Code §1798-1798.78; CSU Code: HR 2005-16 – Requirements for Protecting Confidential Personal Data, HR 2005-01 – Reference to Information Practices Act of 1977; CSUN Policy No. 500-52 – Protection of Confidential Electronic Information

DEFINITIONS:

1. **45 C.F.R. Title 45 CFR Part 46:** Code of Federal Regulations, Title 45 Public Welfare, Department of Health and Human Services, Part 46: Protection of Human Subjects

2. **Biometrics:** the science and technology of measuring human body characteristics

3. **Confidential Information:** confidential business, or financial information provided that the information does not include:

   (a) information that is publicly known or that is available from public sources;
   (b) information that has been made available by its owner to others without a confidentiality obligation; or
   (c) information that is already known by the receiving Party, or information that is independently created or compiled by the receiving Party without reference to or use of the provided information

4. **Critical Data**: information collected under certain prescribed conditions to populate encrypted data fields in the InnoSoft Fusion recreation management system (referred to as SRC Fusion) that includes data from Level I, Level II, and Level III data classifications:
   a) Biometric Data (Handprint Outline) (Level I)
   b) Student/Faculty/Staff/Alumni ID (Level III)
   c) First Name (Level III)
   d) Last Name (Level III)
   e) Middle Name (Level III)
   f) Campus E-mail Address (Level III)
   g) Birth Date (students only) (full mm-dd-yy) (Level II)
   h) Classification (Level II)
   i) Major (Level II)
   j) Gender (Level II)
   k) Employee Status (Full-Time/Part-Time) (Level II)
   l) User ID (Level III)

5. **Data Classification:** the CSU standard of protected data levels.

   a) **Level I (Confidential):** intended solely for use within the CSU and limited to those with a "business need-to know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons outside of

the University is governed by specific standards and controls designed to protect the information.

b) **Level II (Internal):** internal use information is information which must be protected due to proprietary, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights, or make legal action necessary.

   Non-directory educational information may not be released except under certain prescribed conditions. Non-directory student information may not be released except under certain prescribed conditions.

c) **Level III (Public):** information that is generally regarded as publicly available. Information at this level is either explicitly defined as public information or intended to be available to individuals both on and off campus or not specifically classified elsewhere in this standard.

   Knowledge of this information does not expose the CSU to financial loss or jeopardize the security of the CSU's information assets. Level 3 information may be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

   Publicly available data may still be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

6. **Encryption:** a process that takes information and transcribes it into a different form that is unable to be read by anyone who does not have the encryption code. Types include: SQL TDE, and HTTPS (SRC Web site). Fusion will be using SQL Server 2008, which will use AES 128 bit encryption.

7. **InnoSoft Fusion:** a recreation management system designed in partnership with the Student Recreation Center at California State University, Northridge. The name given to the system involved with this project is SRC Fusion.

8. **Record Retention Schedule**: a document identifying a series of unique records/information associated with a corporate process or function. For each record/information listed, the schedule will include a unique number/identifier, title, custodian, value, retention authority, and retention period. The basic schedules are to be modified by each department as needed, e.g., to specify custodians, incorporate additional records, etc.

9. **SSL (**Secure Socket Layer): a cryptographic protocol which provides communications security over networks (Intranet and Internet). SSL is also known as Transport Layer Security (TLS). SSL utilizes symmetric key encryption.

10. **TDE (**Transparent Data Encryption): performs real-time I/O encryption and decryption of the data and log files. The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. TDE protects data "at rest", meaning the data and log files. It provides the ability to comply with many laws, regulations, and guidelines established in various industries.

POLICY:

It is the policy of the University Student Union (USU)/Student Recreation Center (SRC) to maintain records (information) that have been created or received by California State University, Northridge Information Technology (hereafter referred to as Campus IT) or that is collected at the SRC site and downloaded into the InnoSoft Fusion recreation management system (hereafter referred to as SRC Fusion) on behalf of the SRC. Records may be categorized by type, such as SRC, general, fiscal, etc. and shall be retained by the software indefinitely. The SRC has sole custody of this data. It is not accessible to a third party. This policy is designed to ensure compliance with legal and regulatory requirements while implementing appropriate operational best practices.

The policy consists of procedures to promote sound, efficient, and economical data management in the following areas:

I. Creation and organization of records
II. Security, privacy and access to records
III. Rights of access and publication

This policy applies to all USU/SRC administrative records that are stored in SRC Fusion, except as superseded by federal laws, regulations, and USU/SRC contracts.

The USU Executive Director/designee shall be responsible for the ongoing coordination of the records.

Approved by the University Student Union Board of Directors on December 5, 2011.

PROCEDURE:

I. Creation and organization of records

A. The SRC shall use processes developed by Campus IT to download twice each week to SRC Fusion the critical student, faculty, staff and alumni data.

B. Alumni Association IT shall download weekly to SRC Fusion the critical Alumni Association data *(Note: discussions are pending w/the Alumni Association)*.

C. The SRC shall collect on site Level I, II and III data.

D. The SRC shall collect Level III data only on guests who are in high school, elementary school, pre-school children and younger with the consent of a parent or legal guardian.

E. Fusion shall organize data records based on pre-determined encrypted fields as designated by the SRC.

F. The SRC would ask members to voluntarily provide Level III data.

II. Security, privacy and access to records

A. The SRC Fusion system is secured via encryption. Types include: SQL TDE, SSL, and HTTPS (SRC Web site). Fusion encrypts the data as well.

B. Access to Fusion records shall be restricted as follows: (Includes Levels II and III)

a. System Administrators (view/edit – Levels II and III)
b. SRC Staff (view/edit – Level II and III)
c. Student Supervisors (view only – Level II and III)
d. Student Assistants (view only – Level II and III)

C. All users who are granted SRC Fusion access must first read and sign a University Student Union, Inc. Employee Confidentiality Statement.

D. The event log that monitors login activity shall be monitored weekly for malicious login activity.

E. Cameras shall be installed above membership computer stations for security protection.

F. The use of personal cameras, cell phones with cameras or any data/image-capturing device shall be prohibited while accessing and operating SRC Fusion.

G. Confidential Information**.** The USU/SRC shall limit its disclosure of Confidential Information to the amount necessary to carry out its assessments and will place a confidentiality notice on all such information.

H. Protection of Confidential Information. Confidential Information will not be disclosed, copied, reproduced or otherwise made available to any other person or entity without the consent of the USU/SRC except as required by a court or administrative body of competent jurisdiction, or federal law or regulation. The USU/SRC shall use reasonable efforts to maintain the confidentiality of Confidential Information, which will in no instance be an effort that is less than what USU/SRC administrators use to protect their own Confidential Information.

Privacy on Biometrics: The HandKey II which is used for biometric access into the facility does not collect and store an image of the hand, but instead it converts the image to a 9-byte numerical template which is a mathematical representation of size and shape of the hand.

Once this numerical template is developed, it is stored in a memory location which is defined by the person's ID number.

To authenticate a user already verified in the database, the user's ID is entered and the hand is placed on the platen (surface area where users place their hand). An image of the hand is captured and then converted to a 9-byte numerical template. If the new template matches the stored template, the person's identity is verified and the access is granted.

No personally-identifiable characteristics such as scars, marks, tattoos, fingerprints or palm prints are captured or detected by the terminal.

I. **Protection of Focus Group/Assessment Information.** The assessment and development activities to be conducted are not intended to involve human subjects within the meaning of 45 C.F.R. Part 46. Should it become necessary to utilize SRC members for focus groups, the SRC shall identify participant feedback in the aggregate and not identify students by name, Student ID number or any Level I data. Activities conducted will conform to the appropriate federal laws and regulations, including but not limited to all applicable FDA regulations and U.S. Department of Health and Human Services (HHS) regulations relating to the protection of human subjects.

III. Rights of Access and Publication

1. **Right of Access to SRC InnoSoft Fusion Data**. The USU/SRC may access SRC Fusion data for the purposes of SRC-related assessments.

2. **Use of SRC Fusion Data.** The USU/SRC shall be free to utilize SRC Fusion data internally for its own purposes, consistent with its obligation as members of the California State University, Northridge community.

3. **Confidential Information.** The USU/SRC shall limit its disclosure of Confidential Information to the amount necessary to carry out its assessments and will place a confidentiality notice on all such information.

4. **Protection of Confidential Information.** Confidential Information will not be disclosed, copied, reproduced or otherwise made available to any other person or entity without the consent of the USU/SRC except as required by a court or administrative body of competent jurisdiction, or federal law or regulation. The USU/SRC shall use reasonable efforts to maintain the confidentiality of Confidential Information, which will in no instance be less an effort than what USU/SRC administrators use to protect their own Confidential Information.

5. **Publication.** The USU/SRC may publish and make publicly available the results of their assessment and development activities.