Colorado State University Personal Records Privacy and Security Policy
Version 1.0 Approved by ITEC: July 8, 2004
Version 1.1 Approved by ITEC: ???

Introduction

Colorado State University collects personal information of a sensitive nature to facilitate and enable its business/academic functions. Unauthorized access to such information may have many severe negative consequences, including exposing those associated with the university to the risk of identity theft, and adversely affecting the reputation of the University. In addition, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), House Bill 03-1175 (the "non-SSN" legislation), and the Family Educational Rights and Privacy Act (FERPA), and the Payment Card Industry Data Security Standard require various classes of information to be protected from unauthorized access. There already exists a University policy covering IT Security for such information in electronic form (see http://www.colostate.edu/Services/acns/security_policies.html). This policy provides commensurate protection for sensitive information stored in paper and other non-electronic form.

The Office of the Senior Vice President (OSVP) shall be responsible for overseeing the implementation and use of this policy beginning on the effective date of this document.

Definitions

Sensitive personal information includes social security number information, personally identifiable health information, personally identifiable financial information including credit card information, personnel and student performance information, proprietary research and academic information, and any other sensitive personal information that through disclosure may adversely affect an individual and/or the University.

Applicability

These policies encompass best practices that are in general to be applied comprehensively at the University. Units that own the record are responsible for implementing this policy.

Personal Records Security Policy

1. Beginning on the effective date of this policy, the amount of sensitive personal information collected and stored shall be the minimum amount required for the efficient and effective conduct of business and academic functions. In particular, units are responsible for compliance ensuring that all of their forms, paper, non-paper and electronic, are in compliance with this aspect of the policy. Periodically, units shall review their policies, operations, forms, archives and other associated functions to ensure they are in conformance with this aspect of this policy.
2. Access to sensitive personal information shall be limited to only those needing access for legitimate business/academic purposes. Periodically, individual access shall be reviewed to be in conformance with this aspect of the policy.
3. Reasonable and prudent efforts shall be made to isolate and protect sensitive personal information from unauthorized access, for example in locked filing cabinets, behind locked doors, etc.
4. To the extent possible, social security numbers (SSNs) shall not be used as the primary numeric identifier for individuals. Units shall cease using SSNs as primary identifiers as

soon as practicable, and especially after the University transitions centrally from the use of SSNs as primary identifiers. This particular policy applies to all forms of information, both electronic and non-electronic, including identification cards.

Governance of These Policies

The Information Technology Executive Committee (ITEC) is responsible for these policies, including adoption, modification and change. Questions concerning this policy may be directed to Patrick J. Burns, Associate Vice President for Information and Instructional Technology, Patrick.Burns@Colostate.edu, 970.491.5778.