Purpose of This Document

This document is intended to clarify policies and practice for CSU IT staff who have access to CSU information of a sensitive nature, especially information of a personal nature. The overarching intent of this document is to ensure that information remains private and confidential to the maximum extent possible.

Responsibility for this Document

This guideline is the purview of the Information Technology Executive Committee (ITEC). Questions regarding this document should be directed to the Vice President for Information Technology, Patrick J. Burns, Patrick.Burns@ColoState.edu.

Introduction

Colorado State University collects, transmits and stores information of a sensitive nature to facilitate and enable its business/academic functions. Protecting the integrity, privacy and confidentially of such information is fundamental to the conduct of higher education. CSU staff are allowed to use IT systems for personal use, as long as the use is incidental to their job performance and does not increase direct costs for the University. Although the University is subject to the Colorado Open Records Act that requires release of certain types of information, there is much information that is not subject to disclosure. Thus, individuals at CSU have an expectation of privacy of information. In this regard, the University has a published privacy policy (see http://www.colostate.edu/info-privacy.aspx). However, that privacy policy pertains in general to the University's rights and obligations to share and use information.

Contrariwise, the guidelines in this document are intended primarily for IT staff who by virtue of their work responsibilities have access to individuals' information in the conduct of their day to day activities. Indeed, operational staff who are responsible for IT systems, servers and networks typically have access to vast quantities of information stored within systems, and information transmitted across networks. Access to that information is often necessary to their business function. Due to the voluminous amount of information that may be easily accessed, IT staff have a special responsibility to protect individuals' privacy and the confidentiality of information, and these guidelines therefore pertain to IT staff.

Policy and Practice

This section contains elements of policy and practice to be observed by all IT staff at the University, and is to be especially observed by those with expansive access to large quantities of sensitive information.

1. Personal usage – CSU employees are permitted to use CSU IT systems for personal matters, provided that usage is incidental, does not incur additional direct costs, and is

consistent with their performance. Thus, it is permitted for a user to store, access and transmit personal and private information using CSU's IT systems.

2. De minimus access – CSU employees are to access only the minimum amount of information necessary to perform their job function.

3. Form of access – In the event that personal information is accessed, it should be accessed insofar as possible in a form so as to preserve de minimus access, for example, by aggregating data at the highest possible level, or analyzing system/network performance from a quantitative perspective rather than a qualitative aspect based upon the content of the information.

4. Release of information – Notwithstanding personal information accessed by supervisors in the normal course of their employment duties, an individual's personal information is not to be released to anyone without prior and specific authorization from the Office of the General Counsel.

5. Should it be necessary to access an individual's personal and possibly sensitive information in the course of normal duties, IT staff shall attempt to contact the user (e.g. by telephone, IM, or email) and request permission for such access. Should that significantly delay operations or impede progress, IT staff may proceed with the access under the guidelines of this document.

6. In the event of an emergency, or to restore or preserve service, IT staff may access whatever information in their judgment is required to preserve the integrity, functionality and performance of IT systems. However, any information accessed or knowledge gained as a result of that access is not to be shared or released. Rather, in general, that knowledge is to be used only to facilitate operation of the IT environment.

7. In the course of normal job duties, should the information accessed raise suspicions of impropriety, then good judgment should be exercised in deciding whether to pursue the matter further. Matters that are judged serious, e.g. incidents that are likely to become public and besmirch the reputation of the University, life and safety issues, issues where others are affected, e.g. obvious and significant unfairness, should be reported to the supervisor. The supervisor should assess the situation, and engage the Office of the General Counsel if the supervisor wishes to pursue the matter further. Should the matter involve central IT systems or IT security, the Director of ACNS and/or the Vice President for IT should also be engaged. All other matters should be treated in a 'don't ask, don't tell' manner.

Usage of this Policy

Individuals who supervise IT staff who access sensitive information are responsible for ensuring during annual performance reviews that IT staff understand and acknowledge their responsibilities as detailed in this document. This may be accomplished formally or informally, at the discretion of the supervisor.