Information Security Policy Development for Institutions of Higher Education

Regis University
School for Professional Studies
MSCIS Program

Professional Project

Submitted to:
Dan Likarish

Date:
December 29, 2005

By:
Dana DesPlanques
Certification of Authorship page

Regis University
School for Professional Studies
MSCIS Program

Certification of Authorship of Professional Project Work

Submitted to: Professor Dan Likarish

Student’s Name: Dana DesPlanques

Date of Submission: 12/29/2005

Title of Submission:
Information Security Policy Development for Institutions of Higher Education

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for the purpose of partial fulfillment of requirements for the MSC 696 course.

Student’s Signature: Dana DesPlanques
Advisor Approval page

Regis University  
School for Professional Studies  
MSCIS Program

Advisor/MSC 696 Faculty Approval Form

Student's Name: Dana DesPlanques

Professional Project Title:  
Information Security Policy Development for Institutions of Higher Education

Advisor’s Declaration: I have advised this student through the Professional Project Process and approve of the final document as acceptable to be submitted as fulfillment of partial completion of requirements for the MSC 696 course. The student has received project approval from the Advisory Board and has followed due process in the completion of the project and subsequent documentation.

ADVISOR: Dan Likarish, Assistant Professor

SIGNATURE:

DATE:
## Project Paper Revision/Change History tracking page

<table>
<thead>
<tr>
<th>Document</th>
<th>Date Submitted</th>
<th>Date Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract Draft 1</td>
<td>12/10/2004</td>
<td></td>
</tr>
<tr>
<td>Abstract Final</td>
<td>1/3/05</td>
<td>1/13/05</td>
</tr>
</tbody>
</table>
Acknowledgements page

This project has been very challenging and difficult for me to complete. I completed my course work for the MSCIS program in July 2004 and am ashamed that it has taken me this long to submit my project. Completing this project has been a very tough task for me as I am facing the busiest time of my life with many responsibilities both personally and professionally.

I thank my husband, Kevin and two children, Keenan and Sierra for their patience and support. I thank my managers and colleagues at Fort Lewis College for giving me the time and tools to complete my project. I could not have done it without the support of Craig Young, Kerry Vosswinkel, and Cheryl Robertson.
Abstract

Information Security Policy Development for Institutions of Higher Education

A safe and secure computing environment is vital to any institution of higher education. Information systems must provide information with the highest possible levels of integrity, availability, and confidentiality. A comprehensive Information Security Policy is a crucial element of such an environment.

The first phase of this project involves research of current Information Security Policy development methodologies, standards, and best practices. A standard higher education framework is developed and followed in this project. The second phase of this project designs and develops a comprehensive Information Security Policy (the “Policy”) for a sample college (the “College”). The Policy establishes firm standards and procedures to protect the information resources of the College community from threats from both inside and outside of the College. Defining responsibilities, guidelines, and practices will direct the College in preventing, deterring, detecting, responding to, and recovering from information security breaches.
Table of Contents

Title Page .................................................................................................................................1
Certification of Authorship page ...............................................................................................2
Advisor Approval page ...............................................................................................................3
Project Paper Revision/Change History tracking page .............................................................4
Acknowledgements page .........................................................................................................5
Abstract ...................................................................................................................................6
Table of Contents ......................................................................................................................7
None..........................................................................................................................................8
List of Figures / Exhibits / Addenda ............................................................................................8
Chapter One: Introduction / Executive Summary ....................................................................9
  1.1 Statement of the problem to be investigated and goal to be achieved ............................9
  1.2 Relevance, significance or need for the project ...............................................................9
  1.3. Barriers and/or issues ......................................................................................................9
  Elements, hypotheses, theories, or questions to be discussed/answered.............................10
  1.5 Limitations/scope of the project .....................................................................................10
  1.6 Definition of terms .........................................................................................................10
  Summary ................................................................................................................................11
Chapter Two: Review of Literature/Research .......................................................................12
  ............................................................12
  2.1 Overview of all literature and research on the project ....................................................12
  2.2. Literature and research that is specific/relevant to the project ..................................13
  2.3. Summary of what is known and unknown about the project topic .............................13
  2.4. The contribution this project will make to the field .....................................................13
  3.1 Research methods to be used ......................................................................................14
  3.2 Life-cycle models to be followed ..................................................................................14
  3.3. Specific procedures .....................................................................................................14
  3.4 Formats for presenting results/deliverables ..................................................................15
  3.5 Review of the deliverables ............................................................................................15
  3.6 Resource requirements .................................................................................................16
  3.7 Outcomes ......................................................................................................................16
  3.8 Summary ......................................................................................................................16
Chapter Four: Project History .................................................................................................17
  4.1. How the project began .................................................................................................17
  4.2. How the project was managed .....................................................................................17
  4.3. Significant events/milestones in the project ................................................................17
  4.4. Changes to the project plan ........................................................................................17
  4.5. Evaluation of whether or not the project met project goals .......................................17
  4.6. Discussion of what went right and what went wrong in the project ............................18
  4.7. Discussion of project variables and their impact on the project .................................18
  4.8. Findings/analysis results .............................................................................................18
  4.9. Summary of results ....................................................................................................18
Chapter Five: Lessons Learned and Next Evolution of the Project ........................................19
  5.1. What you learned from the project experience .............................................................19
  5.2. What you would have done differently in the project ................................................19
Because each higher education institution varies in size, complexity, and culture, Information Security Policies are most effective when they map an individual institution’s needs. This project provides an example of one institution based on its needs. These policies offer guidance directed at ensuring legislative compliance, protecting College assets, and ensuring confidentiality and privacy. Many federal and state laws have been enacted over the past few years in response to the explosion of electronic information. These laws have greatly increased the rules under which institutions of higher education must operate, presenting a challenge for institutions to keep their security policies current. The potential legal exposure and liability are significant, and Information Security policies must be shaped to ensure compliance while reflecting the needs of the institution. Information Technology policies should be a statement of an institution’s values and uphold its mission. They should be designed to protect the rights of individuals and the organization. They have a direct impact on an institution’s public image and form the very foundation on which all Information Security efforts are built.

List of Tables

None

List of Figures / Exhibits / Addenda

6.3.1. Standard higher education framework for the development of an information security policy.

6.3.2. Fort Lewis College Information Technology Security Policy

6.3.3. Fort Lewis College Acceptable Use of Information Technology Policy

6.3.4. Fort Lewis College Information Technology Privileged Access Agreement

6.3.5. Fort Lewis College Data Classification Guidelines
Chapter One: Introduction / Executive Summary

1.1 Statement of the problem to be investigated and goal to be achieved

Information Technology is ever-changing. With unprecedented opportunities for communication, comes the same level of opportunities for risks. A comprehensive information security policy can effectively address the risks to information systems and provide a foundation for mitigating security concerns and incidents. The goal of this project is to develop an effective information security policy that will address the information security challenges of institutions of higher education and provide a roadmap for effectively protecting the availability, integrity, and confidentiality of their systems.

1.2 Relevance, significance or need for the project

Conventional security methods by technical means are simply insufficient for the protection of an organization’s information systems. Information security must be taught to all users of an information system and enforced through a comprehensive information security policy.

1.3 Barriers and/or issues

Information security policies are difficult to enforce. One of the major barriers is the lack of both management and employee support. Although the process of policy development and approval resides with management, maintenance of the policy requires continued recognition and support from both management and employees. If management does not express support for the policy, it is highly unlikely that staff will. Endorsement and continued support by the President is necessary for the college community to take notice.

Political limitations are another inherent challenge in higher education. If the information systems are working and the institution is not in the news, why worry about it? Will this security policy restrict our intellectual freedom? Effective policy marketing, communication, and training are integral pieces to the success of the project.

Information security policies must adhere to the laws and principles of both the organization and the government. Policy rules must be clearly defined to avoid legal implications if a breach of security occurs.

Financial limitations are a continuing challenge in higher education. Organizations often do not allocate the financial means necessary for implementing and maintaining an effective information security policy. With the best intentions of providing the highest level of information security possible, IT professionals are always challenged by the bottom line. Hard work, creativity, and knowledge of the specific financial barriers can help to reduce the impact.

With the ever-changing nature of technology, an effective information security policy must be reviewed, revised, and updated on a regular basis. A policy that is not maintained will simply become worthless.

Information security policies must be carefully crafted to reflect the mission of the organization. Without this synergy, the policy will not succeed.
Elements, hypotheses, theories, or questions to be discussed/answered

This project describes and defines the elements and responsibilities required to create safe and secure Information Systems for all members of the community. The purpose of the Policy is to protect information resources from threats from both inside and outside of the College by setting forth responsibilities, guidelines, and practices that will help the College prevent, deter, detect, respond to, and recover from exploitations of the resources. The Policy is intended to be an enabling mechanism for fostering an environment of secure dissemination of information.

1.5 Limitations/scope of the project

These guidelines apply to all students, faculty, visiting faculty, staff, guests, and external individuals or organizations that use computing and electronic communications resources, and computing equipment owned, leased or rented by the College. Computing equipment includes, but is not limited to, dialup modems, terminals and microcomputers in public labs, minicomputers, telephones, file servers, and networking equipment used to link these components together and to the Internet.

1.6 Definition of terms

Information - Stimuli that have meaning in some context for its receiver. When information is entered into and stored in a computer, it is generally referred to as data. [http://searchsqlserver.techtarget.com/sDefinition/0,290660,sid87_gci212343,00.html]

Information technology – Contemporary term that describes the combination of computer technology (hardware and software) with telecommunications technology (data, image, and voice networks) (Systems Analysis and Design Methods 707)


Information security – Something that gives or assures safety and protection of information

Virus - Program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document. [http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci213306,00.html]

Trojan horse - Program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage. [http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci213221,00.html]

Worm - A self-replicating virus that does not alter files but resides in active memory and duplicates itself. [http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci213386,00.html]

Spyware - Any technology that aids in gathering information about a person or organization without their knowledge. [http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci214518,00.html]

Malware - Any program or file that is harmful to a computer user. [http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci762187,00.html]
Confidential data – Data that shall only be viewed by the owner of the data or those given explicit permission to the data

Internal use only data – Data that should only be viewed within the institution in which it was created

Unrestricted data – Public data

Encryption - the conversion of data into a form that cannot be easily understood by unauthorized people [http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci212062,00.html](http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci212062,00.html)

**Summary**

Institutions of higher education must recognize the extraordinary role information plays in their educational, research, operational, and community outreach missions. A safe and secure computing environment is crucial for any institution of higher education. The Information Systems at any College are vital to the welfare of the institution. Information Systems must provide information with the highest possible levels of integrity, availability, and confidentiality. A comprehensive Information Security Policy is a key element of such an environment.
Chapter Two: Review of Literature/Research

2.1 Overview of all literature and research on the project

ISO 17799: Pay Attention to this One

JISC : BS7799 Pilot
www.jisc.ac.uk/uploaded_documents/ACFRCAhGaydY.ppt

Strategies for Crafting Effective Security Policies
http://www.checoweb.org/Spring2003/CIO_presentation2.ppt

Georgetown University Information Security Policy
http://uis.georgetown.edu/policies/technology/secpol.html

University of California, Berkeley – Campus Information Technology Security Policy
http://security.berkeley.edu:2002/IT.sec.policy.html

Protecting Your Information
http://www.jisc.ac.uk/index.cfm?name=event_protecting_1099

BS7799 / ISO 17799 Methodology
http://www.bs7799-2.net/index.html

Information Security Management: BS 7799.2:2002 Audit Checklist
www.sans.org/score/checklists/ISO_17799_checklist.doc

Achieving Best Security Practices Utilizing ISO 17799 Standards
http://documents.iss.net/marketsolutions/ISOMatrix.pdf

The Security Risk Management Guide
http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx


http://www.rusecure.co.uk/download_page.htm

JISC Generic Information Protection (Security) Policy
www.jisc.ac.uk/uploaded_documents/sec_policy.rtf


University of Minnesota - Acceptable Use of Information Technology Resources
http://www.fpd.finop.umn.edu/groups/ppd/documents/policy/Acceptable_Use.cfm

Developing an Information Security Policy
http://www.jisc.ac.uk/index.cfm?name=jcaspapers_security

Computer and Network Security in Higher Education
2.2. **Literature and research that is specific/relevant to the project**

See Section 2.1

2.3. **Summary of what is known and unknown about the project topic**

The need for information security standards and policies is a known fact wherever information technology exists. Information technology is ever-changing and pieces of the future of information security are unknown. Ongoing diligence and research are necessary to protect our information systems from the dangers of the unknown.

2.4. **The contribution this project will make to the field**

This project will contribute to the information security initiative at Fort Lewis College, the sample college. The author’s hope is that other institutions of higher education will benefit from this project.
Chapter Three: Methodology

3.1 Research methods to be used
1. Documentation review – Use Internet resources to study best practices and existing policies. Use textbooks to study definitions and theory.
2. Institutional policy review – Learn from common practices of the institution in order to create a policy supportive of the needs of the institution.
3. Case studies – conduct a comprehensive examination of information technology policies and procedures.
4. Focus groups – join an information security focus group to explore the topic in depth through group discussions.

3.2 Life-cycle models to be followed
The SANS security Life Cycle Model will be followed (http://www.sans.org/rr/whitepapers/testing/260.php):

The steps in the Security Life Cycle Model include:
1. Assess – The overall security health of the system is evaluated.
2. Design – Design a security configuration that will support the standards of both the institution and the industry.
3. Deploy – Implement based on the design developed. Approval and management buy-in are essential.
4. Manage and Support – Ongoing step crucial to the longevity of the security system.

Education is a fundamental component of the Security Life Cycle Model. Education is continuous and ongoing throughout all steps of the Life Cycle.

3.3 Specific procedures
Procedures are equally important as policies. Policies often define what is to be protected and the ground rules. Procedures outline how to protect the resources or how to carry out the policies. The procedures of this methodology follow the ISO 17799 Best Practices. Each item below should be addressed in each step of the Security Life Cycle Model:

1. Information Security Policy
   A. Organizational security
B. Information Security infrastructure
C. Security of third party access
D. Outsourcing

2. Asset Classification and Control

3. Personnel Security
   A. Security in job definition and resourcing
   B. User training
   C. Responding to security incidents and malfunctions

4. Physical and Environmental Security
   A. Secure areas
   B. Equipment security
   C. General controls

5. Communications and Operations Management
   A. Operational procedures and responsibilities
   B. System planning and acceptance
   C. Protection against malicious software
   D. Housekeeping
   E. Network management
   F. Media handling and security
   G. Exchanges of information and software

6. Access Control
   A. Business requirement for access control
   B. User access management
   C. User responsibilities
   D. Network access control
   E. Operating system access control
   F. Application access control
   G. Monitoring system access and use
   H. Mobile computing

7. Systems Development and Maintenance
   A. Security requirements of systems
   B. Security in application systems
   C. Cryptographic controls
   D. Security of system files

8. Business Continuity Management
   A. Aspects of business continuity management

9. Compliance
   A. Compliance with legal requirements
   B. Reviews of security policy and technical compliance
   C. System audit considerations

3.4 Formats for presenting results/deliverables
   During the approval portion of the deployment phase, deliverables shall be presented through presentations during formal meetings. Final deliverables shall be presented in both online and paper format.

3.5 Review of the deliverables
   See Section 4.9.
3.6 Resource requirements

1. Human resources – Staff must be assigned and committed to the task of developing the system. Depending on the size and state of the information security systems in place, staff time for assessment, design, and deployment could be as little as a few hours a week for a few months or as much as several hours a week for up to a year. Management, support and ongoing training should have time of at least a few hours per week permanently.

2. Financial resources – Tools to implement effective information security systems require significant financial resources. Budgets can vary significantly based on organizational size and implementation methods.

3. Technical resources – A technical infrastructure capable of supporting and servicing the tools is essential to the success of an effective information security program.

3.7 Outcomes

The outcome of the project will be an effective information security policy that addresses the information security challenges of institutions of higher education and provides a roadmap for effectively protecting the availability, integrity, and confidentiality of their systems.

3.8 Summary

The methodology employed in this project provides for a thorough process upon security policy development with the aim of making the most secure information systems possible. This process with a strong emphasis on planning is essential to the success of the project.
Chapter Four: Project History

4.1 How the project began
I applied for the Networking Lab Practicum in July 2003 before my MSCIS course work was complete. At the time, I thought that I was on track to become a Network Administrator at Fort Lewis College. I began working on a remote network administration project. In May 2004, I was convinced by my Director to pursue a different direction toward management of technology. I spoke with Dan Likarish about the possibility of redesigning my project and he had an open mind to which ever track I decided to choose. I wanted to select a topic that I could begin for my MSCIS degree and continue to work on through my career with Fort Lewis College. I sat down with my Director and asked for suggestions. He had plenty. We discussed thin client computing, anti-pest systems, copyright protection systems, server consolidation, integrated messaging, survey systems, self-defending networks, and finally a comprehensive information security policy. We discussed how each option would fit my skills and interests as well as the urgency and longevity of each option. I decided that developing an information security policy would best suit my interests.

4.2 How the project was managed
I began researching and working on the project alone. The more I read, the more I realized that good policies are produced when a team or task force is formed. I believe my Director realized this at the same time and he assigned one of his managers the task of working with me to get the job done by September 1, 2005. The Manager of Information Systems has been the unofficial security guru of IT at FLC for several years. In April 2005, she and I began meeting every two weeks and I was able to learn from her so that I could progress forward to my final goal.

I was also asked to join a Security Group with other members of the IT department. We meet monthly to discuss, prioritize, and act upon information security issues and concerns.

4.3 Significant events/milestones in the project
Teaming up with the Manager of Information Systems and becoming part of the Security Group were significant milestones for me. She has become a mentor for me with her vast knowledge of information security, college policies, and state and federal laws.

4.4 Changes to the project plan
This project began as research and development of an Information Security Policy. Upon researching our current policies, we realized that other Information Technology policies, plans, and agreements needed to be addressed. Therefore, the project plan grew into a complete review and redesign of all Information Technology policies.

4.5 Evaluation of whether or not the project met project goals
As of today, I am very pleased with the outcome of the policy development project with Fort Lewis College. In all honesty, my main goal with Regis is to receive credit for my work and finally earn my diploma. I have planted a seed in my career with Fort Lewis College with this project and I plan to continue working on it for many years to come. Information Security is the direction in which I would like to point my career. My ultimate goal of this project is to challenge myself intellectually while providing my employer with the best level of information security possible.
4.6 Discussion of what went right and what went wrong in the project

I feel great about the product I have created. My Director has reviewed it and is very pleased as College officials very interested in addressing these policies. I am excited about being a part of the review and implementation phases of the policies. I feel that my contribution will be acknowledged and hopefully respected.

As of now, I do not feel that anything necessarily went wrong in the project.

4.7 Discussion of project variables and their impact on the project

Not applicable

4.8 Findings/analysis results

Not applicable

4.9 Summary of results

Following is a summary of the work:

<table>
<thead>
<tr>
<th>New Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security</td>
</tr>
<tr>
<td>Acceptable Use of Information Technology</td>
</tr>
<tr>
<td>Information Technology Administration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Changed Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-1 - Computer Account Use</td>
</tr>
<tr>
<td>6-17 - Electronic Communications</td>
</tr>
<tr>
<td>These two policies have been chopped up. Appropriate parts have been moved to new Acceptable Use Policy. What was left was combined to create new Information Technology Administration Policy.</td>
</tr>
</tbody>
</table>

| 6-6 - Use of Student Residence Computer Networks |
| 6-8 - Student Instructional Computing Responsible Use Code |
| 6-18 - Connecting Computer and Network Devices to the Campus Network |
| All contents of these three policies have been moved to the new Acceptable Use Policy. Some portions that are no longer applicable have been deleted. |

<table>
<thead>
<tr>
<th>Other New Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged Access Agreement (for IT staff)</td>
</tr>
<tr>
<td>Data Classification Guidelines</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Documents to be Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Impact Analysis</td>
</tr>
<tr>
<td>Risk/security assessment</td>
</tr>
<tr>
<td>Risk management process</td>
</tr>
<tr>
<td>According to Information Security Policy, these three documents are to be completed by Summer 2006.</td>
</tr>
</tbody>
</table>

Security Awareness Program:
http://www.fortlewis.edu/administrative_services/it/security/securityhome.asp
Chapter Five: Lessons Learned and Next Evolution of the Project

5.1 What you learned from the project experience
The main lesson I learned in this project is that developing comprehensive policies is not a one person job. It is a very difficult task that requires collaboration and insight from many individuals in various areas of expertise.

5.2 What you would have done differently in the project
Accepting the limited resources that I have before me, I would not change anything in the project.

5.3 Discussion of whether or not the project met initial project expectations
This project met my expectations.

5.4 What the next stage of evolution for the project would be if it continued.
The next stage of the project will be to go through the policy approval process. Once approved, a marketing and awareness program will be launched for the College community. All policies will be reviewed annually and revised as needed.

Business Impact Analysis, Risk/security assessment, and Risk management process documents will be completed by summer 2006.

5.5 Conclusions/recommendations
I understand the importance of a comprehensive Information Security Policy and related documents. For the protection of the availability, integrity, and confidentiality of any information system, I highly recommend the development and acceptance of such a Policy.

5.6 Summary
Because each higher education institution varies in size, complexity, and culture, Information Security Policies are most effective when they map an individual institution’s needs. This project provides an example of one institution based on its needs. These policies offer guidance directed at ensuring legislative compliance, protecting College assets, and ensuring confidentiality and privacy.

Many federal and state laws have been enacted over the past few years in response to the explosion of electronic information. These laws have greatly increased the rules under which institutions of higher education must operate, presenting a challenge for institutions to keep their security policies current. The potential legal exposure and liability are significant, and Information Security policies must be shaped to ensure compliance while reflecting the needs of the institution.

Information Technology policies should be a statement of an institution’s values and uphold its mission. They should be designed to protect the rights of individuals and the organization. They have a direct impact on an institution’s public image and form the very foundation on which all Information Security efforts are built.
Chapter Six - Back Matter

6.1 References / Bibliography


http://www.rusecure.co.uk/download_page.htm


http://www.giac.org/certified_professionals/practicals/gsec/3778.php

http://www.jisc.ac.uk/index.cfm?name=jcas_papers_security

The Joint Information Systems Committee (JISC). “JISC Generic Information Protection (Security) Policy”.  
www.jisc.ac.uk/uploaded_documents/sec_policy.rtf

www.sans.org/score/checklists/ISO_17799_checklist.doc


http://security.berkeley.edu:2002/IT/sec.policy.html

http://www.it.ufl.edu/policies/security/

http://www.fpd.finop.umn.edu/groups/ppd/documents/policy/Acceptable_Use.cfm

Williams, Jane. “Protecting Your Information”. 15 October 1999  
http://www.jisc.ac.uk/index.cfm?name=event_protecting_1099
6.2 Exhibits/Addenda

6.2.1 Information Security Policy Framework

**Security Assessment**
1. Learn the goals of the organization
2. Identify all assets
3. Identify likely threats
4. Identify possible controls
5. Define roles and responsibilities

**Policy Construction**
1. Write policy based on findings from security assessment.

**Policy Implementation**
1. Publish and advertise the policy
2. Educate users on the elements of the policy

**Policy Maintenance**
1. Ongoing seminars and awareness campaigns
2. Scheduled monitor and review
6.2.2

INFORMATION TECHNOLOGY SECURITY POLICY

I. PURPOSE

This Policy describes and defines the elements and responsibilities required to create safe and secure Information Systems for all members of the community. The purpose of the Policy is to protect information resources from threats from both inside and outside of the College by setting forth responsibilities, guidelines, and practices that will help the College prevent, deter, detect, respond to, and recover from exploitations of the resources. The Policy is intended to be an enabling mechanism for fostering an environment of secure dissemination of information.

II. AUTHORITY

This section will include the College officers that have authorized this policy.

III. SCOPE

These guidelines apply to all students, faculty, visiting faculty, staff, guests, and external individuals or organizations that use computing and electronic communications resources, and computing equipment owned, leased or rented by Fort Lewis College. Computing equipment includes, but is not limited to, dialup modems, terminals and microcomputers in public labs, minicomputers, file servers, and networking equipment used to link these components together and to the Internet.

IV. GENERAL

According to the Federal Critical Infrastructure Assurance Office, an Information System is defined as:

“All electronic and human components involved in the collection, processing, storage, transmission, display, dissemination, and disposition of information.”


Fort Lewis College (the “College”) recognizes the extraordinary role information plays in the College’s educational, research, operational, and community outreach missions. A safe and secure computing environment is crucial for any institution of higher education. The Information Systems at the College are vital to the welfare of the institution. Information Systems must provide information with the highest possible levels of integrity, availability, and confidentiality. A comprehensive Information Security Policy is a key element of such an environment.

As mandated by the State of Colorado, the College utilizes a layered security approach to protect its Information Systems. This Policy includes, but is not limited to, these eight components:

1. Business Impact Analysis - document to be completed by Summer 2006
2. Risk/security assessment - document to be completed by Summer 2006
3. Risk management process - document to be completed by Summer 2006
4. Contingency plan for disaster recovery/business continuity
5. Security safeguards for asset protection
6. Secure architecture design
7. Security awareness and training programs
8. Monitor/audit system
V. ROLES AND RESPONSIBILITIES

All members of the College community share in the responsibility for protecting information resources for which they have access. Responsibilities vary depending upon the role of the user.

A. Roles

1. **Users**
   All Members of the College community with a computer account are users. Users include faculty, staff, students, authorized volunteers, community members, and visitors. All Stewards, Managers of Users, Information Technology Personnel, and the Information Security Officer are Users. Their responsibilities cover both computerized and non-computerized information and information technology devices that are in their care and possession.

2. **Managers of Users**
   Members of the College community with management or supervisory responsibility, including Vice Presidents, Deans, department chairs, directors, and supervisors are Managers of Users.

3. **Stewards**
   Members of the College community who have the primary responsibility for particular information are Stewards. A few examples would be:
   - a. The Controller is the Steward of the College’s financial data.
   - b. The Registrar is the Stewards of student registration data.
   - c. Faculty members are Stewards of their research and course materials.
   - d. Students are Stewards of their own work.

4. **Information Technology Personnel**
   Members of the Office of Information Technology manage significant information resources and systems for the purpose of making those resources available to the College community. Information Technology Personnel face more extensive requirements than individuals for information security. Beyond providing access and protecting against unauthorized use and physical threats, they must play a more proactive role in implementing and enforcing security policies and procedures.

5. **Information Security Officer**
   The individual designated in writing by the Vice President of Finance and Administration with the primary responsibility for oversight of information security, networks and systems, security policy, and educating the College community about security responsibilities.

B. Responsibilities (by Role)

1. **Users** are responsible for:
   
   a. Reading, understanding and complying with the [Acceptable Use of Information Technology](#) policy.
2. **Managers of Users** are responsible for:

a. Ensuring that the people they manage or supervise have access to the information needed to perform their jobs.

b. Requesting access from the Stewards of the information resources.

c. Maintaining, adjusting, and/or requesting removal of access for Users when their job responsibilities change or when their employment is terminated.

d. Ensuring that any specific information security policies and procedures they establish for the people they manage or supervise are consistent with this Policy, as well as with other College Policies, and laws.

3. **Stewards** are responsible for:

a. Determining the classification of their information as Confidential, Internal Use Only, or Unrestricted. Labeling of both physical and electronic information is encouraged to clearly identify the classification, where possible.

b. Determining who is authorized to have access to their information. Directing the Office of Information Technology to grant or remove access for users. Ensuring that those with access have a need to know the information to perform their job. Informing users of the classification of the data they have access to and the security requirements for that data.

c. Collaborating with the Office of Information Technology to establish specific information security policies and procedures for the information resources they manage, including procedures related to the creation, retention, distribution, and disposal of information. Such policies and procedures must be consistent with this Policy, as well as with other College Policies and laws.

4. **Information Technology Personnel** are responsible for:

a. Providing and maintaining a secure network architecture. Elements of design shall include, but are not limited to firewalls and intrusion detection and prevention devices.

b. Ensuring that the Information Technology infrastructure of the College (including, but not limited to servers, network switches, routers, cables) is physically secured. Power, temperature, water, and fire monitoring devices shall be in place as appropriate. Locks, cameras, alarms, etc. shall be installed in critical areas to discourage and respond to unauthorized access to the electronic or physical components.

c. Backing up College data stored on network servers on a regular schedule. Schedules, retention periods, and storage facilities shall provide for restoration of data following disaster or corruption. Backup processes shall conform to the record keeping requirements as identified by the data.
Stewards. Frequency of backups will be determined by a risk assessment process, and may range from continuous to no more than weekly. Backup media are to be stored in a secure location. Data on backup media should be encrypted, where possible.

d. Implementing technologies, designs, policies, and procedures that protect the confidentiality, integrity and availability of College information, in general following currently accepted industry best practices. Examples include but are not limited to:
   i. Properly configuring operating systems and other software to reduce vulnerabilities to a minimum.
   ii. Updating software in a timely fashion to alleviate security vulnerabilities as they arise.
   iii. Providing software that detects, removes, and prevents the spread of malware such as viruses, worms, Trojan horses and spyware.
   iv. Periodically probing the network for vulnerabilities, using software tools designed for this purpose.
   v. Using available software features to require strong passwords, and requiring Users to change initial passwords upon first use. Requiring proper identification before resetting forgotten passwords.

e. Ensuring that College information systems are in compliance with published security standards that the College is legally bound by. Such standards may include but are not limited to FERPA, HIPPA, and credit card acceptance security standards such as CISP and SDP.

f. Auditing systems to detect intrusions. This includes monitoring event logs, examining performance data, and using other available tools and procedures to check for any evidence of unauthorized access, the presence of viruses or other malicious code, or any other indicators of confidentiality or integrity loss.

g. Responding to security incidents in an appropriate and timely fashion. This includes but is not limited to:
   i. Reporting suspected or known compromises of information resources to the College Information Security Officer
   ii. Preserving and protecting evidence and cooperating with authorized investigations
   iii. Locking or revoking accounts
   iv. Restricting network access for individuals or computing devices
   v. Restoring compromised college-owned equipment to a clean, functional, malware-free state. Installing additional security measures where needed to protect against future compromises.
   vi. Treating security incidents as Confidential.

h. Ensuring that all data storage media are electronically sterilized using currently accepted industry standards before disposal. If electronic sterilization methods are not available or practical, such devices will be destroyed in such a method as to prevent retrieval of data.

i. Granting individuals access privileges to information resources. In circumstances where the data being accessed is controlled by a data Steward, such access will not be granted without receipt of written
permission from the Steward. In time-critical situations, verbal authorization may be accepted but must be confirmed by a written authorization within a reasonable time period.

j. Providing information security and awareness training for all members of the College community, and informing them of their responsibilities as Users, Stewards, Managers, and Information Technology Personnel.

k. Understanding, agreeing to and complying with the Fort Lewis College Privileged Access Agreement.

5. The Information Security Officer is responsible for:

   a. Staying abreast of Federal, State, and local legislation and how it affects security policy and planning. Monitoring activities and best practices relating to security at institutions of higher education.

   b. Overseeing all information network and system security. The Information Security Officer has authority for temporary implementations that deviate from this Policy in emergency situations or until the policy can be reviewed.

   c. Overseeing all stages of security incident responses. Depending on the nature of the incident, this can involve collecting and analyzing evidence, determining the responsible party, assessing damages, restoring data from backup files, closing security holes, installing stronger security measures, revising security guidelines and procedures, taking disciplinary action in accordance with appropriate College policies and reporting incidents to law enforcement. The Information Security Officer will coordinate with all other necessary members of the College community.

   d. Overseeing the Security Training and Awareness program.

   e. Establishing procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements.

   f. Contingency Planning. This includes but is not limited to:
      i. Creating and maintaining a Disaster Recovery plan that details procedures for the resumption of mission critical business information services following the loss of equipment and/or data. Printed copies of this Internal Use Only document are stored in the office of Information Technology and distributed to internal IT Managers for off-site storage.
      ii. Participating in the College business continuity planning process.
      iii. Periodic review of procedures for backup and restoration of College data.

VI. POLICY COMPLIANCE AND ENFORCEMENT

A. Policy audit.

The Information Security Officer shall determine whether information is being
protected in conformance with this Policy and with other College policies.

B. Enforcement.

The Information Security Officer shall oversee the enforcement of this Policy. Violations shall be handled consistent with College disciplinary procedures. The College may temporarily suspend, block or restrict access to information and network resources if necessary in order to protect the integrity, availability, and/or confidentiality of College information or to protect the College from liability. The College may refer suspected violations of applicable law to appropriate law enforcement agencies.

VII. REVIEW AND REVISION

The Information Security Officer shall assess this Policy annually to determine if revisions are needed to accommodate the fast changing nature of information technology or weaknesses in the Policy.
Acceptable Use of Information Technology

I. PURPOSE
The computing and electronic communications resources at Fort Lewis College (FLC) support the instructional, research, and administrative activities of the College. Users of these facilities may have access to College resources, sensitive data, and external networks. Consequently, it is imperative for all users to behave in a responsible, ethical, and legal manner. This policy presents specific guidelines to appropriate behavior and use of FLC computing resources which are designed to contribute to the security and stability of the network.

II. AUTHORITY
This policy was reviewed and approved by <fill in here>

III. SCOPE
These guidelines apply to all students, faculty, visiting faculty, staff, guests, and external individuals or organizations that use computing and electronic communications resources, and computing equipment owned, leased or rented by Fort Lewis College. Computing equipment includes, but is not limited to, dialup modems, terminals and microcomputers in public labs, telephones, minicomputers, file servers, and networking equipment used to link these components together and to the Internet.

IV. ACCEPTABLE USE
Those who make use of the Fort Lewis College computing network are required to behave in a manner consistent with Fort Lewis College's codes of conduct (See Student and Employee Handbooks). As a user of this network, you agree to the following usage guidelines:

1. General
   a. Read, understand and adhere to all College Information Technology policies and exercise good judgment in the protection of information resources.
   b. Fort Lewis College is not responsible for the content of any material you prepare, receive, transmit, or store. Thus, as a condition of using the College's computer system, you represent that you are in compliance with all federal, state and international copyright and other intellectual property laws, licensing agreements and other federal and state laws, and that you will not use the system to violate any federal, state or local civil or criminal laws. Furthermore, you will indemnify, exonerate and save the College (and its representatives) harmless from any claim, damage or cost related to your use, including any legal fees the College decides it is necessary to incur to defend itself.
   c. Because anti-virus programs cannot provide 100% protection from malicious software, you agree to exercise due caution when opening Email, browsing the Internet, downloading files from the Internet, and installing software. You should avoid opening unexpected or suspicious attachments.
   d. Immediately report any suspected or known information security compromises, including viruses or malicious code, on a system under your control to Information Technology personnel (as listed at
http://www.fortlewis.edu/administrative_services/it/contact.asp) and to cooperate with internal or external investigations if requested.

e. Take advantage of security training opportunities that are offered by the College to maintain awareness of current security issues.

f. Conduct all communications from off campus in a secure manner. Secure access can be achieved by:
   1. Dialing in to the campus modem pool
   2. Using a Virtual Private Network (VPN) connection
   3. Communicating via web pages that utilize protocols such as SSL / TLS to encrypt data during transmission. (e.g. a URL beginning with https:// uses a secure protocol.)

2. Computer Accounts

Computer accounts are granted to Fort Lewis College faculty, staff, and students for bona fide purposes related to their work or studies at the College. You are responsible for all activities, including electronic mail transmissions, associated with any computer account you have been given, whether such activities are performed by you or by another person using your account.

The Office of Information Technology cannot retrieve lost or forgotten passwords. A new password will be issued upon presentation of a valid picture ID to either the Helpdesk or a Lab Coordinator.

a. Make appropriate use of account protection features such as selecting a secure password that is not easily guessed and changing your password at regular intervals.

b. Use only those computer accounts that have been created for your use. The negligence of another user in revealing an account name or password is not considered authorization for use.

c. If you have reason to believe that someone has made unauthorized use of your account, immediately change your password and report the incident to the Office of Information Technology.

d. If you are the head of a department that has been assigned a group account – for example, an email account for an entire office – you are responsible for all use of the account. You agree to notify the Office of Information Technology when a group account is no longer needed.

3. Individually Assigned Computing Resources

a. Physically protect the resources under your control. For example, doors shall be locked to protect equipment when unattended. Particular care is expected when traveling and at home to protect these devices.

b. Make your systems available for anti-virus and operating system updates, patches, and service packs.

c. Be responsible for backing up any data stored on your computer. Backup media containing Confidential or Internal Use Only data must be stored securely, using encryption or password protection on the documents or media.
4. Shared Computing Resources

Computers located in labs require a logon, and are available to registered students, staff, and faculty of Fort Lewis College. Kiosks located in areas such as building corridors and the Library do not require a logon and may be available to the general public.

a. Observe posted closing times, and to vacate labs at non-posted times when requested to do so. Facilities have varying priorities for use, described fully in the Computer Lab Use and Scheduling Policy. All users should leave prior to the posted beginning of these classes, unless otherwise permitted by the instructor.

b. Comply with guidelines posted in the public computing facilities (e.g. no smoking, eating, drinking, chewing tobacco).

c. Log off from applications, computers, and networks located in computer labs or other public areas or when finished. When using on or off campus public facilities such as Internet kiosks where logging off is not allowed, you should always close your Internet browser(s) if possible when finished with your session.

5. Non-College-Owned Devices Attached to the Network

The College computer network is a shared, finite resource installed by the College to promote scholarship and learning. Accidental or intentional disruption of the network will deprive others of access to important College resources. College and internet resource access typically requires computer account authentication.

a. Be responsible for the security of any computer system or network device you attach to the network, and for any intentional or unintentional activities from or to that network connection.

b. Comply with all policies governing the use of network resources, including but not limited to the Student Conduct Code and the Information Technology Security Policy.

c. To avoid network conflicts that arise when duplicate computer names appear on the network, use the name assigned to your Windows® computer by the Office of Information Technology. If you are a student and wish to connect your personal computer to the network, set your Computer Name to your Fort Lewis College network account username.

d. Run a legally licensed operating system that is approved by the Office of Information Technology. Contact the Office of Information Technology for a current list of approved operating systems. If not on the approved list, it will be your responsibility to demonstrate that the system is up-to-date with regard to security patches, antivirus software updates, firewall services and other standard security measures.

c. Run a current version of a College-approved antivirus software package. Contact the Office of Information Technology for a current list of approved vendors. Students, Faculty and Staff of Fort Lewis College may obtain antivirus software free of charge that is licensed by the College. Antivirus software must be configured to receive automatic updates of virus definition files on at least a weekly, and preferably a daily basis. Scans should be run at least weekly.
f. Update your computer operating system and application software regularly to maintain the current level of Service Packs, patches, hotfixes, or other software updates related to security and network stability.

g. Make your device available for scanning and update to meet the College’s required security standards, including but not limited to patch levels, service pack versions, definition files, and scan engines.

h. In the event that the Office of Information Technology issues a notice requiring the installation, either immediately or within a designated time period, of a specific security update that is deemed to be critical to the continued security and stability of the network, you agree to apply the update within the time frame specified. Assistance with the installation of such critical updates will be provided if possible. You understand that computers found to be non-compliant may be disconnected from the network if necessary.

i. If a system you attach to the network creates security problems or disrupts others’ use of the network, your device will be disconnected until the problems are remedied.

V. UNACCEPTABLE USE

The following activities are strictly prohibited. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. You may be exempted from these restrictions during the course of your legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

1. General

   a. Under no circumstances are you authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Fort Lewis College owned or leased resources.

   b. State of Colorado Fiscal Rule forbids use of State equipment or resources for private purposes.

   c. Examining, copying, modifying or deleting files and/or data belonging to other users without their prior consent.

   d. Using Fort Lewis College computer systems and/or networks to attempt to gain unauthorized access to remote systems.

   e. Making any intentional attempts to obtain unauthorized access to or otherwise interfere with the operation of network systems or programs.

   f. Willfully introducing computer “malware” (e.g. viruses, worms, spyware or other disruptive/destructive programs) into the College network or into external networks.

   g. Intentionally operating any network-intensive application which overloads the network. If you are notified of such an application detected running on a computer under your control that is impeding other users through mass consumption of system resources, you agree to discontinue running the software. If the application presents an imminent hazard to the College network or disrupts the activities of others, the offending computer system or the subnet to which it is attached may be disconnected without prior notice.
h. Performing any unauthorized, deliberate action which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction.

i. Executing port scans, security scans, or any form of network monitoring which will intercept data not intended for you, unless this activity is a part of your normal job duty.

j. Forging or attempting to forge electronic mail messages or header information.

k. Attempting to read, delete, copy, or modify the electronic mail of other users.

l. Sending or attempting to send harassing, obscene, or other threatening e-mail to another user.

m. Making illegal copies of software licensed to the College.

n. Using College-owned computer accounts, computer and communications equipment, software, and networks for commercial purposes. These purposes may include, but are not limited to:
   1. Sending Unsolicited Commercial Email (UCE, more commonly known as spam), other “for profit” messages, or chain letters.
   2. Transmission of commercial or personal advertisements, solicitations, or for extended reproduction of political, ideological or commercial material originated by a person or organization.
   3. The execution of revenue-generating advertising programs.

o. Using software and hardware provided by the College for work outside the teaching, learning, and professional mission of the College. Incidental and occasional personal use not related to College business may be permitted if it does not materially interfere with the availability of services for College purposes and does not result in a direct cost for the College. (For example, receiving an incidental electronic mail message electronically does not create a direct cost; printing a personal electronic mail message does.)

p. Modifying configuration options or installing additional software that may cause increased security vulnerabilities. Installing software or devices to allow remote access to a College-owned computer in such a way that would bypass existing security measures.

q. Encroaching on other’s use of shared computing resources. Such encroachment shall include, but is not limited to, creating a disturbance, displaying offensive material on shared equipment, or otherwise interfering with others’ use of shared computing resources.

r. Pointing a non-fortlewis.edu domain name at a host within the Fort Lewis College address space, unless that domain is being used by a recognized college organization or affiliate, and the domain registration is handled or approved by the Office of Information Technology.

s. Offering “server-class” services from your device without prior approval from the Office of Information Technology. Examples of such “server-class” services
include, but are not limited to: DNS, DHCP, SMTP (e-mail), WINS, File and Print Sharing, WWW (web services such as Microsoft IIS or Apache).

t. Connecting any wireless access devices to the campus network without prior approval from the Office of Information Technology. The Office of Information Technology will collaborate with the person or group affected to ensure that security is maintained and that no interference is introduced into existing systems.

2. Computer Accounts

a. Attempting to decrypt system or user passwords.

b. Attempting to secure a higher level of privilege on network systems, or attempting to subvert the restrictions associated with your use of accounts and/or software.

c. Revealing your account password to others, except for the purpose of technical support by Information Technology personnel. If you must share your password with Information Technology personnel for technical support, you agree to change your password upon resolution of the technical issue. You agree not to store or post your password in any manner, electronic or physical, that would make it easily accessible to unauthorized users.

d. Allowing use of your account by others. This includes family and other household members.

VI. PRIVACY AND CONFIDENTIALITY

1. Information Handling

a. You are responsible for knowing the privacy and confidentiality restrictions associated with any information to which you have access. You agree to safeguard information that is classified Confidential or Internal Use Only, as defined in the Information Technology Security Policy and the Data Classification Policy. Such safeguards include but are not limited to:

1. Storage of information:
   a. Storing such information in a place that provides a high level of protection against unauthorized access. In general, this means on secure network drives (e.g. "M:" or "O:" drives) as provided by the Office of Information Technology.
   b. Not taking such information outside of the College unless it can be assured adequate protection. Ensuring that all such data that is taken outside the College is stored in an encrypted format.
   c. Logging off or locking devices containing Confidential or Internal Use Only data when left unattended.

2. Distribution and transmission of information.
   a. Not distributing nor making Confidential or Internal Use Only information available to persons who are not authorized to access the information. This applies to originals, copies, and new materials that contain all or part of the information, and to oral communication of information. When Confidential and Internal use only information is
distributed, it shall be distributed in such manner that the future distribution restrictions are clear.

b. Appropriately protecting Confidential or Internal Use Only information that is transmitted electronically, transported physically, or spoken in conversation from unauthorized interception. Encryption shall be used when electronically transmitting Confidential information. In general, electronic mail is not appropriate for transmitting Confidential information. Tamper-resistant packaging shall be used when physically transmitting Confidential information.

3. Destruction and disposal of information and devices.
   a. Disposing of Confidential or Internal Use Only information on paper or other physical media in such a manner as to ensure that it cannot be retrieved and recovered by unauthorized persons. Confidential or Internal Use Only documents must not be placed in recycling bins. Paper shredders are highly recommended.
   b. Taking care to ensure that Confidential or Internal Use Only data is rendered unreadable when disposing of computers or removable media.

2. Electronic Communications and Data
   a. The College does not routinely intercept or monitor electronic mail, other electronic communications, or other data stored in electronic format. Capture and/or "reading" of electronic communications and/or other data stored in electronic format by technical staff or others is expressly prohibited, except under the following circumstances:
      1. To resolve technical or delivery problems.
      2. To prevent illegal, unauthorized, or inappropriate use.
      3. To meet externally imposed legal requirements.
      4. In the course of an investigation triggered by indications of misconduct.
      5. To protect health and safety.
      6. To prevent interference with the mission of the College.
      7. To locate information required for College business that is not more readily available elsewhere.

   b. The College reserves the right to disclose the contents of staff, faculty, student, and other authorized users' electronic communications or other data stored in electronic format without permission of the user, but will do so only when it has a legitimate business need and only with explicit authorization from the president or the appropriate vice president. The College will attempt to refrain from disclosure that would result in personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

   c. You agree that electronic mail, other electronic communications, or other data stored in electronic format on College business or with the use of College resources may be made available for review by any authorized College official for purposes related to College business.

   d. Employee correspondence in the form of electronic mail may be a public record under the public record law and may be subject to public inspection under section 24-72-203 of the Colorado Revised Statutes.

   e. The Family Educational Rights and Privacy Act of 1974 (FERPA) gives students the right to inspect and review their educational records and provides them with
some protection against the release of information. Electronic correspondence could become a student record under FERPA, and thus be available to disclosure under that Act.

f. Confidentiality regarding student records is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA). All use of electronic mail, including use for sensitive or confidential information, will be consistent with FERPA.

3. Confidential Data

a. You agree to comply with:

1. The Family Educational Rights and Privacy Act (FERPA) of 1974 (Buckley Amendment), as amended. If your account gives you access to student data, you must comply with all FERPA regulations regarding disclosure of student information. To find out specifically what information you may or may not give out and to whom, visit the FERPA website maintained by the Records office or contact that office via phone or e-mail. When you are in doubt as to whether or not you are permitted to release some information, do not release the information until you know for sure.

2. The laws of the State of Colorado, the United States and other regulatory agencies. This includes all applicable federal and state laws which govern the privacy and confidentiality of data, including but not limited to the Electronic Communications Privacy Act of 1986, Health Insurance Information Portability and Accountability Act (HIPAA), Foreign Corruptions Practice Act, Gramm-Leach-Bliley Act, and the Computer Fraud and Abuse Act.

3. All College policies and handbooks.

VII. CONSEQUENCES OF POLICY VIOLATIONS

1. Malicious, destructive or illegal conduct or failure to comply with this policy may result in disconnection from the network, loss of lab privileges, legal action, or other disciplinary action, subject to normal College procedures as described in the appropriate student, faculty or employee handbooks and documents. Illegal activities may be reported to the appropriate civil authorities for prosecution. The College will fully comply with the authorities to provide any information necessary for the litigation process.

2. The Office of Information Technology may revoke accounts at any time if computing privileges are abused. This revocation may be temporary, if such action is deemed necessary for the successful management and operation of the facilities, or permanent through the normal College disciplinary process.

3. You are responsible for any damages resulting from your failure to comply with these guidelines. Such damages include the cost of College staff time spent recovering from any unauthorized activity.

4. Faculty and staff will be referred to their dean or department head for appropriate action. Students will be subject to normal College disciplinary procedures as outlined.
in the student handbook.

5. Copyright violation procedures:
Storing or transmitting content in violation of federal, state and international copyright and other intellectual property laws and agreements and other federal and state laws will result in the following disciplinary action:
   i. Faculty and staff will be referred to their dean or department head for appropriate action.
   ii. Students in the Residence Hall network will be subject to the following rules:

   a. 1st Offense
      a. Port will turned off until workstation is compliant
      b. Student informed of offense and compliance requirements
      c. Computer is inspected for compliance ~ port turned on
      d. User is referred to Judicial Affairs
      e. Documentation of student incidents is shared with student and parents as allowed by FERPA and other applicable law

   b. 2nd Offense
      a. Port will be turned off for an indefinite period of time
      b. Student informed of offense and compliance requirements
      c. Computer is inspected for compliance ~ port turned on after punitive period
      d. User is referred to Judicial Affairs
      e. Documentation of student incidents is shared with student and parents as allowed by FERPA and other applicable law

   c. 3rd Offense
      a. Port will be turned off for remainder of semester
      b. Student informed of offense and compliance requirements
      c. Computer is inspected for compliance ~ port turned on the first day of the following semester
      d. User is referred to Judicial Affairs
      e. Documentation of student incidents is shared with student and parents as allowed by FERPA and other applicable law
Office of Information Technology
Privileged Access Agreement

The Office of Information Technology must grant Information Technology personnel privileged access to the College’s information systems in order to provide technology services to the students, faculty, and staff of Fort Lewis College. Privileged access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. This access imposes responsibility and obligation upon the Information Technology employee to use the systems in an ethical, professional, and legal manner that is strictly within his or her authorized job functions.

In exchange for the privileges granted as an employee of the Office of Information Technology, you agree to abide by the following standards:

1. To use your privileged access account(s) only when broad access is required. Normal accounts, without broad privilege, shall be used in the ordinary performance of duties, whenever such accounts provide the means to accomplish the job.

2. To use your privileged access only to perform assigned job duties. Examples may include:
   - Relocating files when systems are upgraded, repaired, or replaced.
   - Performing repairs required to return a system to normal function, such as fixing files or file processes, or killing runaway processes.
   - Running security checking programs.
   - Accessing user data to the extent necessary to resolve a problem.
   - Remotely accessing user’s desktops with their permission for the purpose of solving a problem.
   - Granting, changing, or denying resources, access, or privilege to another individual following existing organizational guidelines and procedures.

3. Not to violate end user privacy by accessing contents of electronic email or files except where necessary to resolve a problem or comply with legal requirements.

4. To take every reasonable precaution to:
   - Prevent unauthorized access to any passwords, user identifications, or other information that may be used to access the systems.
   - Prevent unauthorized access to information contained in or obtained from the systems.
   - Protect the confidentiality of information encountered in the performance of your duties. If you inadvertently see information possibly indicating inappropriate use, you shall consult with your supervisor or other available authority.

5. Not to share, copy, transmit, alter, or delete information in these systems except when required to perform your duties.

6. To obtain permission from the Steward of the data before altering or deleting the data. Under most circumstances, the consent of the account owners should be obtained, if possible, before accessing their files or interfering with their processes. However, if good faith efforts to obtain consent are not successful and changes are necessary to maintain acceptable system performance, actions may be taken without consent and you will notify the affected individual of the action(s) taken and the reasons for the action(s) taken as soon as possible.
7. To pass along to another IT employee any support request that might give you privileged access to your own academic scores or to an electronic course in which you are enrolled.

8. To seek guidance from your Information Technology Manager whenever you are unsure of the correct decision regarding appropriate use, confidentiality, or access, and do so BEFORE you take any action on the support issue in question.

9. To report any incidents of non-compliance with the terms of this agreement to your Information Technology Manager.

The Office of Information Technology is committed to advancing the ethical and responsible use of all information systems, and will not tolerate illegal, dishonest, improper, or irresponsible use. Any violation of these standards is a serious offense and may result in disciplinary action up to and including termination of your employment at the College. Illegal activities may be reported to the appropriate civil authorities for prosecution.

By signing below, you acknowledge that you have read and will comply with this Privileged Access Agreement, the Acceptable Use of Computing Resources and Electronic Communications Policy, and the Information Technology Security Policy.

____________________________________  __________________________________________
Employee                                      Date

____________________________________  __________________________________________
Information Technology Manager                  Date
DATA CLASSIFICATION GUIDELINES

I. PURPOSE

The Information Systems at Fort Lewis College are essential to the educational, research, informational and operational functions of the College. These systems and the data contained within them must be protected from accidental and/or intentional misuse. The College must provide information with the highest possible levels of integrity, availability, and confidentiality. Fort Lewis College is committed to putting forth its best effort in protecting its information resources from accidental or intentional intrusion or damage. The College is equally committed to preserving and nurturing the open, information-sharing requirements of its academic culture.

Information resources are considered to be assets of the College. Protecting information assets is driven by a variety of considerations:

A. Legal - There are laws, both federal (e.g., HIPAA, FERPA) and state (e.g., social security number use, credit card exposure), that mandate the level of protection the College is required to provide.

B. Academic - The College both produces and owns intellectual capital which needs to be protected against premature disclosure or unauthorized tampering.

C. Financial - There are costs directly related to the protection of information assets. Similarly, there are costs directly related to the control and repair of damage to information resources which have been compromised.

D. Other Business Requirements - The College strives to make information resources widely available while putting forth a best effort to keep private things private. In addition to the direct costs related to loss or compromise of data, Fort Lewis College’s reputation as an institution is something that, if damaged, can have both direct and indirect negative effects.

II. Classification of Assets

Information assets are classified according to the risks associated with the data being stored or processed. Data with the highest risk needs the greatest amount of protection to prevent compromise.

A. The three levels of data (or asset) classification are:

1. Confidential - Requires the highest level of protection. Data whose loss, corruption or unauthorized disclosure would impair the business or research functions of the College, result in any business, financial, or legal loss, or be a violation of federal or state laws/regulations or College contracts.
   
   a. Confidential Data may be disclosed to individuals on a need-to-know basis only.
   
   b. Information in this category may be released to internal parties of the College only when specifically authorized in writing by the
appropriate Data Steward or other specifically authorized College agent.

c. Information in this category may be disclosed to parties outside the College only when specifically authorized in writing by the appropriate Data Steward or other specifically authorized College agent when the external party is under contractual obligation of confidentiality with the College and/or under the written instruction of the Office of the President.

d. When stored in an electronic format, Confidential data must be protected to prevent loss, theft, unauthorized access and unauthorized disclosure and must be encrypted and/or password protected when not in use.

e. Confidential data must not be disclosed to parties without explicit permission of the appropriate Data Steward, Vice President, or the President.

f. Access control measures to Confidential data must afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.

g. Confidential information will not be posted on any public website.

h. The appropriate Data Steward and the Office of Information Technology must be notified in a timely manner if data classified as Confidential is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of College’s information systems has taken place or is suspected of taking place.

2. **Internal Use Only** – Data whose loss, corruption or unauthorized disclosure would not necessarily result in any business, financial or legal loss but which is made available to Data Steward approved users only.

a. Internal Use Only is the default classification for data.

b. Internal Use Only data is information that is confidential to members of the College community who have a legitimate need to access such data.

c. Data classified as Internal Use Only must not be disclosed to parties external to the College or parties internal to the College without permission of the appropriate Data Owner.

d. Data in this category must be protected from unauthorized access, modification, transmission, storage or other use.

3. **Unrestricted** - The lowest level defined. Data that do not fall into any of the other data classifications.
a. Unrestricted data may be made generally available without specific Data Steward approval.

b. Unrestricted data is available to all members of the Fort Lewis College community and to all individuals and entities external to the Fort Lewis College community.

B. College procedures regarding data security and classification shall:

1. Comply with and be based on the laws of the State of Colorado and the United States, and such regulatory agencies as these laws empower. This includes all applicable federal and state laws which govern the privacy and confidentiality of data, including but not limited to the Electronic Communications Privacy Act of 1986, Family Educational Rights and Privacy Act of 1974 (as amended).

2. Apply to all data created and maintained by the College (i.e. student, research, financial, payroll/personnel, etc.) except where superseded by grant or other contracts, or by federal Copyright Law.

3. Include all College data regardless of the medium on which it resides (e.g., paper; fiche; in electronic form on tape, cartridge, disk, CD-ROM, or hard drive; etc.) and regardless of form (e.g., text, graphics, video, voice, etc.).

C. Data is often kept in collections called databases, tables, files, etc. In the design of most systems, more sensitive data elements of a collection are not usually segregated from less sensitive elements. Therefore, in determining the classification category, it is the most sensitive data element in the collection which determines the classification category of the entire collection.

D. The table and examples below can be used as a guide to determine the appropriate category of any particular data collection. A positive response to the highest category in any row is sufficient to place that system into that Classification.

<table>
<thead>
<tr>
<th>Legal requirements</th>
<th>Confidential Data (highest, most sensitive)</th>
<th>Internal Use Only Data (moderate level of sensitivity)</th>
<th>Unrestricted Data (low level of sensitivity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of data is required by law (e.g., see list of specific HIPAA and FERPA data examples)</td>
<td>Fort Lewis College has a contractual obligation to protect the data</td>
<td>Protection of data is at the discretion of the owner or Data Steward</td>
<td></td>
</tr>
<tr>
<td>Reputation risk</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Other Institutional Risks</td>
<td>Information which provides access to resources, physical or virtual</td>
<td>Smaller subsets of protected data from a school or department</td>
<td>General College information</td>
</tr>
<tr>
<td>Access</td>
<td>Only those individuals designated with approved access and/or signed non-disclosure agreements</td>
<td>Fort Lewis College employees and non-employees who have a business need to know</td>
<td>Fort Lewis College affiliates and general public with a need to know</td>
</tr>
</tbody>
</table>
E. More specific examples of Confidential Data:

1. **HIPAA - Protected Health Information**
   - Patient Names
   - Social security numbers
   - E-mail, URLs, & IP #'s
   - Account/Medical record #'s
   - Certificate/license #'s
   - Device id's & serial #'s
   - Full face images
   - Payment Guarantor's information
   - Street address, city, county, zip code
   - Telephone/Fax #'s
   - Dates (except year) for dates related to an individual
   - Health plan beneficiary numbers
   - Other unique identifying number, characteristic, or code
   - Biometric identifiers
   - Vehicle id's & serial #'s

2. **FERPA - Student Records** (For more information, see Fort Lewis College's [FERPA web page.](https://www.fortlewis.edu/ferpa))
   - Grades
   - Student Financial information
   - Credit Card Numbers
   - Bank Account Numbers
   - Wire Transfer information
   - Payment History
   - Financial Aid / Grant information
   - Student Tuition Bills

   The following “directory information” may be revealed by the College without student consent unless the student designates otherwise.
   - Student's Name
   - Addresses
   - Telephone Numbers
   - Fort Lewis College E-mail Address
   - Date and Place of Birth
   - Major and Minor Fields of Study
   - Dates of Attendance
   - Degree Information (including degree and date conferred, honors, awards information, scholarships and academic awards)
   - Class and Enrollment Status
   - Participation in Recognized College Activities and Sports
   - Most Recent School Attended

3. **Donor Information**
   - Name
   - Graduating Class & Degree(s)
   - Credit Card Numbers
   - Telephone/Fax #s
   - E-Mail, URLs
   - Employment information
4. **Research Information**
   - Funding / Sponsorship information
   - Human subject information
   - Lab animal care information

5. **Employee Information**
   - Social Security Number
   - Payroll information
   - Name
   - Date of birth
   - Home address or personal contact information
   - Benefits information
   - Performance reviews
   - Worker’s compensation or disability claims

6. **Business data**
   - Credit card numbers
   - Bank account information
   - Purchasing card numbers
   - Social Security or other Taxpayer ID numbers
   - Contract information (between FLC and third parties)

7. **Management data**
   - Monthly Expenditure Statements
   - Detailed annual budget information
   - College’s investment information
   - Employee evaluations

III. **RESPONSIBILITIES**

Responsibilities vary depending upon the role of the user. All Users of the College Information Systems have responsibilities as described in the College Information Security Policy, the Acceptable Use of Information Technology Policy, and other applicable College policies. Data Steward responsibilities are particularly important in regard to these guidelines. In addition to other responsibilities, the Data Stewards of the College are responsible for classifying data and authorizing appropriate access.

IV. **COMPLIANCE AND ENFORCEMENT**

Any individual found misusing data, divulging confidential data or otherwise violating these Guidelines may be denied or given limited access to data and/or College information systems, and shall be subject to reprimand, suspension, dismissal, legal action, and/or other disciplinary action. Any known violations of these Guidelines must be reported to the College's Information Security Officer and the relevant Data Steward.