OFFICE OF INFORMATION TECHNOLOGY
Policies and Procedures Manual

1.1. Appropriate Use and Information Security/Confidentiality Policy

1.1.1. Approval and adoption

1.1.1.1. Approved by the Chief Information Officer and Executive Vice President and adopted effective 10/15/2002.

1.1.1.2. Changes made to clarify “Procedures” and “Enforcement” sections. Approved by the Chief Information Officer and Executive Vice President and adopted effective 12/5/2002.

1.1.1.3. Addition of articles 1.1.3.4.14 and 1.1.3.4.15 and a modification of article 1.1.3.4.12 to enforce student firewall pinholing. Approved by the Chief Information Officer and Executive Vice President and adopted effective 8/31/2004.

1.1.1.4. Expanded article 1.1.3.2 to clarify electronic and physical storage and handling of confidential information, with special emphasis on Social Security Numbers. Approved by the Chief Information Officer and Executive Vice President and adopted effective 7/28/2005.

1.1.1.5. Further expanded article 1.1.3.2 to include all data elements deemed confidential based on curr2(sla Pres8.1(asuch ased byents)]TJ13j-9 -1.15 TD0 Tc

1.1.2.2. To protect the integrity, security, and confidentiality of data and/or information stored on University of La Verne computing systems.

1.1.2.3. Appropriate use of information technology resources at the University of La Verne includes instruction, independent study, authorized research, independent research, and official work of the offices, units, recognized student and campus organizations, and agencies of the University.

1.1.3. Policy

1.1.3.1. Users who maintain or access data or information contained in electronic form in the University's computing systems must:

1.1.3.1.1. follow standard security practices such as maintaining password secrecy and logging out of accounts when not in use;

1.1.3.1.2. use it only as required in the performance of their jobs;

1.1.3.1.3. disclose confidential information to other staff on a need-to-know basis; and

1.1.3.1.4. exercise due and diligent care to protect data and information from unauthorized access, use, disclosure, alteration, or destruction.

1.1.3.2. Users are responsible for complying with all applicable laws and regulations regarding the dissemination and protection of data and information that is confidential, particularly with regards to the Family Educational Rights and Privacy Act of 1974 (FERPA) - also known as the Buckley Amendment, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLB), and any other applicable state and federal legislation dealing with information privacy.

1.1.3.2.1. Under no circumstances shall student, alumni, or employee data designated as confidential be extracted and/or stored on computer systems external to the University of La Verne's enterprise databases maintained by the Office of Information Technology (BANNER, BiTech, and Viking) without express written permission from the University Registrar and the Chief Information Officer. Confidential data elements covered by this policy include:

1.1.3.2.1.1. **Social Security Numbers**

1.1.3.2.1.2. **Birthdates**
1.1.3.2.1.3. **Driver's License Numbers**
1.1.3.2.1.4. **Credit Card Numbers**
1.1.3.2.1.5. **Bank Account Numbers or Routing Information**

1.1.3.2.2. Printed reports containing one or more of the data elements listed above may only be created and printed by the office responsible for the data (Registrar for student data, University Relations for alumni data, and Human Resources for employee data). These reports shall be used in a "need to know" manner and shall be kept in a confidential environment. Paper reports containing Social Security Number(s) or other confidential information may not be thrown in the trash, but should be shredded (not by hand) or returned to the originating office for proper disposal.

1.1.3.2.3. Faculty or staff maintaining databases and/or copies of printed reports containing Social Security Number(s) or other confidential information are personally responsible for abiding by FERPA, HIPAA, and other state and federal regulations.

1.1.3.3. Institutional data (generally data required for use by more than one organizational unit and relevant to planning, managing, operating, controlling, or auditing administrative functions of an administrative or academic unit of the University), including any and all student related records, shall be stored on computers owned and operated by the University of La Verne unless express permission has been granted to do otherwise by the Chief Information Officer in the Office of Information Technology.

1.1.3.4. Although not exhaustive, the following list emphasizes activities that are NOT allowed on University of La Verne networks or computer systems. No University computing facility or service or any other University computing asset will be used in any illegal activity, including but not limited to:

1.1.3.4.1. conduct or behavior that is prohibited by University policies including harassment or hate crimes as defined in these policies and state and federal laws and regulations;

1.1.3.4.2. commercial activity not authorized in writing by an Officer of the University;

1.1.3.4.3. accessing or distributing any type of illegal pornography;

1.1.3.4.4. the "hacking" of any computer system;

1.1.3.4.5. distributing or making unauthorized use of any data, information stored in the computing systems;

1.1.3.4.6. knowingly recording any inaccurate or false data in University records;

1.1.3.4.7. using or having others use University technology for personal business;

1.1.3.4.8. giving their passwords or access to any other person (University or outside personnel);

1.1.3.4.9. making, distributing, or using unauthorized or illegal copies of licensed and/or copyrighted software, media, or material;

1.1.3.4.10. obstructing others' work or access by consuming large amounts of system resources such as disk space, CPU time, and network bandwidth;

1.1.3.4.11. knowingly introducing destructive software such as programming loops or "viruses" into the system, or running Internet file-sharing applications (such as Napster, Morpheus, KaZaA, etc.) which provide "stealth" sharing services to the world;

1.1.3.4.12. attempting to circumvent or subvert any system's security measures or resource allocations (Residence Hall computers using firewalls must have the firewall "pinholed" to enable network access for the University's network monitoring tools - used only to detect network policy violations);

1.1.3.4.13. disrupting service, detrimentally impacting bandwidth, or intentionally damaging files, hardware, or software belonging to the University of La Verne;

1.1.3.4.14. installing a router, wireless router, or wireless access point on any University network (including the Residence Halls) without written approval from the OIT Network Team; and

1.1.3.4.15. creating a hostile or intimidating work or academic environment through the personal viewing of sexually explicit or offensive materials in the workplace or computer labs.

1.1.3.5. In cases of doubt, it is the users responsibility to inquire with the Chief Information Officer in the Office of Information Technology concerning the permissibility of technology use.

1.1.3.6. With reference to discovery or access by the University, there shall be no user confidentiality as to any information contained or transmitted by any University computing facility or service or any other University computing asset.

1.1.3.7. Proprietary information is stored on or transmitted using any University computing asset at the risk of the user; the University cannot assure that such proprietary information will remain private or confidential.

1.1.4. Procedure

1.1.4.1. Any user who discovers unauthorized access attempts or other improper usage of University of La Verne technology should report the infraction the Chief Information Officer in the Office of Information Technology, or other appropriate administrator.

1.1.4.2. Management personnel are responsible for ensuring employees and students are aware of and trained in the provisions of this policy.

1.1.5. Enforcement

1.1.5.1. Employee violations of any part of this policy will result in disciplinary action up to and including dismissal.

1.1.5.2. Student violations of any part of this policy will result in disciplinary action up to and including suspension or expulsion.

1.1.5.3. Authorized access to networks, systems, data, and information is a privilege granted to individuals to perform their University duties. Misuse of this access could result in the loss of this privilege and therefore the inability to perform one's job. By using University of La Verne computing systems and signing the Appropriate Use statement users signify understanding and acceptance of the policies outlined therein.