UNIVERSITY of LOUISIANA Lafayette Information Technology

Comprehensive Information Security Program

Table of Content

1 Introduction

1.1 UL Lafayette Information Security Strategy Purpose

The purpose of UL Lafayette's Information Security Strategy is to support and coordinate our university community to secure UL Lafayette Information and Information systems from cyber attacks while complying with legal, statutory, contractual, and internally developed requirements.

Using the ISO 27002 security standard as the guideline, this document will define control objectives, identify and assess approaches to meet the objectives, select controls, establish benchmarks and metrics, and describe implementation and testing plans.

1.2 ISO 27002 Security Standards Background

The security standard ISO1799 was originally prepared by British Standard Institute as BS 7799, adopted by the Joint Technical Committee ISO/IEC JTC1, and approved by The International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC).

BS 7799 was issued to provide a set of controls comprising best practices in information security. It is a strong reference point for identifying the range of controls needed for most situations where information systems are used in the business world. The standard is being worked through the ISO acceptance process is the ISO 27002 standard.

1.3 The Control Triad – Preventive, Detective and Corrective

According to the Institute of Internal Auditors, there are three categories of controls - preventive, detective and corrective.

Preventive Controls are designed to reduce the likelihood that information will be lost or changed through unauthorized access, disclosed to unauthorized individuals, accidentally or intentionally modified or deleted.

Preventive controls also limit the impact of lost productivity by ensuring the continued availability of information. Preventive controls include:

- Administrative controls such as employee orientation, confidentiality agreements, and separation of duties
- Processes such as communication with information owners and stewards regarding information sensitivity, communications with end users regarding software updates, change control for technical architecture, testing backups, examining logs, and periodic vulnerability scanning of servers
- Technical measures such as firewalls, eliminating unneeded services, and backups

Detective Controls enable the detection of problems when they are small, reducing losses. Detective controls are needed because preventive controls are never 100% effective, and because the preventive controls needed, may change from day to day. When detective controls are implemented effectively, managers should expect to see an increase in the number of incidents detected. Although the implementation of detective controls will result in an increase in the number of incidents, early detection will reduce the severity and impact of these incidents. A host-based intrusion detection system (IDS) is an example of a detective control.

Corrective Controls enable recovery when the failure of a preventive control is detected. Antivirus

solutions often provide an all-in-one package of preventive, detective, and corrective (file cleaning) capabilities. Corrective actions may also include restoring systems from system images, restoring data from backups, and investigations/forensics. Planning for compromises is a prerequisite of effective corrective measures.

1.4 Selection of Controls

The selection of controls will be grounded in a cost comparison of different strategic approaches to risk mitigation. The cost comparison will contrast the costs of various approaches with the perceived gains UL Lafayette could realize in terms of increased confidentiality, availability, or integrity of systems and data. Those gains could include reduced financial losses, increased university community confidence, positive audit findings, and regulatory compliance. Any particular approach will consider: (1) policies, standards, and procedures; (2) technology and architecture; (3) resource dedication; (4) training; and (5) testing.

1.5 Layering of Controls/Defense In Depth

Excessive reliance on a single control could create a false sense of confidence. Therefore, the UL Lafayette Information Security Strategy requires multiple layers of security controls and testing to establish several lines of defense between the attacker and the asset being attacked. To successfully attack the data, each layer should be penetrated. With each penetration, the probability of detecting the attacker increases.

2 Role and Responsibilities

All members of the University community share in the responsibility for protecting information resources for which they have access or custodianship. Most of the responsibilities set forth in this section are assigned to four groups of people: Stewards, Users, Managers (of Users), and Information Custodians. In general, an individual will have responsibilities in more than one area. This section also articulates specific responsibilities for the University IT Security Officer, Local Information Security Analysts, the Internal Audit Department, and the University Operational Review

2.1 Owner

The University is considered the INFORMATION OWNER of all university information; individual units within the institution may have stewardship responsibilities for portions of the information.

2.2 Stewards

Stewards are those members of the University community who have the primary responsibility for particular information. Each type of "production system information" needs a Steward. One becomes the Steward either by designation or by virtue of having acquired, developed, or created information resources for which no other party has stewardship. For example, the Campus Librarians are the Stewards of the library catalogs and related records; and the Registrars of the University are the Stewards of student data. For purposes of the Information Security Policies, faculties are considered the Stewards of their research and course materials; students are considered the Stewards of their own work.

Stewards have the responsibility of Users of their information. In addition, they are responsible to perform the following activities:

- **Establishing security policies and procedures**. Stewards may establish specific information security policies and procedures for their information where appropriate. Stewards are responsible for the procedures related to the creation, retention, distribution and disposal of information. These should be consistent with the University Information Security Policies, and the University's Records Retention Policy, as well as with other University policies, contractual agreements, and laws. Stewards may impose additional requirements that enhance security.
- **Assigning classification**. Stewards are responsible for determining the classification of their information and any specific information handling requirements that go beyond the University Information Security Policies, particularly as may be imposed by confidentiality agreements with third parties. Information that is Confidential or Internal-use-only shall be marked as such when it is presented or distributed to Users, especially when failing to do so could lead to a misunderstanding of the classification. Additional markings specifying handling and distribution requirements may be added
- **Determining authorizations.** Stewards determine who is authorized to have access to their information. They shall make sure that those with access have a need to know the information and know the security requirements for that information. For Confidential information, they should also make sure that those given access have a need to know and have signed a confidentiality agreement that covers the information. Information may be disclosed only if disclosure is consistent with law, regulations and internal University policies, including those covering privacy. Except under unusual and specifically recognized circumstances, access shall be granted to individuals in such manner as to provide individual accountability.

- **Record Keeping.** Stewards shall keep records documenting the creation, distribution, and disposal of Confidential information. This process is also recommended for other types of information.
- **Incident reporting.** Stewards shall report suspected or known compromises of their information to their Managers, the University IT Security Officer, and/or Local Information Security Analists. Incidents will be treated as Confidential unless there is a need to release specific information. Stewards should designate a back-up person to act if they are absent or unavailable. Stewards may not delegate ownership responsibilities to third party organizations (such as outsourcing firms) or to any individual who is not a full-time UL Lafayette employee. When both the Steward and the back-up Steward are unavailable, pressing Steward decisions may be made by the Department Head who ordinarily handles the information.

2.3 Users

Every University community member is an information resource User. Users include, for example, students, faculty, staff, contractors, consultants, and temporary employees. Users are required to abide by all security requirements defined by Stewards, implemented by Custodians, and/or established by the IT Security Office. Users are required to familiarize themselves with, and act in accordance with all UL Lafayette information security requirements. Users are also required to participate in information security training and awareness efforts. Users should request access from their immediate manager, and report all suspicious activity and security problems.

2.4 Managers

Managers are members of the University community who have management or supervisory responsibility, including deans, department chairs, directors, group leaders, supervisors, etc. Faculty who supervise teaching and research assistants are included. Managers have all the responsibilities of Users and, where information resources originate, Stewards. In addition, they share responsibility for information security with the people they manage and supervise. They also are responsible for the following:

Establishing security policies and procedures. If Managers decide to establish specific information security policies and procedures for the people they manage or supervise, these should be consistent with the University Information Security Policies, as well as with other University policies, contractual agreements, and laws.

Managing authorizations. Managers should make sure their people have the access authorizations needed to perform their jobs. The authorizations themselves are acquired from the Stewards of the information resources. Managers should make sure their people lose access when they are terminated or job responsibilities change. Managers are responsible for administering and retaining confidentiality statements for the people they manage or supervise if confidentiality statements are required by the Steward(s) of the information.

User training and awareness. Managers shall provide an environment that promotes security. They shall make sure their people have the training and tools needed to protect information.

Incident handling and reporting. Managers shall report suspected or known compromises of information resources, including contamination of resources by computer viruses, to their Managers, the University IT Security Officer, and/or Local Information Security Analyst. They shall cooperate with the investigation of and recovery from security incidents, including taking any disciplinary action deemed necessary by the appropriate University authorities. Incidents will be treated as Confidential

unless there is a need to release specific information.

2.5 Custodians

Custodians are in physical or logical possession of information and/or information systems. Like Stewards, Custodians are specifically designated for different types of information. In many cases, a Department Head or a Director in the Technology Services Department will act as the Custodian. If a Custodian is not clear based on existing information systems operational arrangements, then the Chief Information Officer will designate a Custodian. Custodians follow the instructions of Stewards, operate systems on behalf of Stewards, but also serve Users authorized by Stewards. Custodians should define the technical options, such as information criticality categories, and then allow Stewards to select the appropriate option(s) for their information. Custodians also define information systems architectures and provide technical consulting assistance to Stewards so that information systems can be built and run to best meet business objectives. If requested, Custodians additionally provide reports to Stewards about information system operations, information security problems, and the like. Custodians are furthermore responsible for safeguarding the information in their possession, including implementing access control systems to prevent inappropriate disclosure, as well as developing, documenting, and testing information systems contingency plans.

2.6 Local Information Security Analysts

Local Information Security Analysts are appointed by Information Custodians from those campuses, schools, departments and individuals that manage significant information resources and systems for making those resources available to others. The appointed personnel are responsible for extending information security within their organization to systems and networks that they manage. Often they will have first-hand knowledge of their specific configurations and applications that will necessitate further definition of policies and procedures at their organizational level. They will provide user education and training. They will work closely with the University IT Security Officer to ensure that the University Information Security Policies are implemented and enforced consistently across the University. They will take steps to remediate, respond to and recover from a security incident, similar to the way the University IT Security Officer is authorized to do so. Local Information Security Analysts should notify the University IT Security Officer of all incidents and actions taken.

2.7 IT Security Office

The IT Security Office is the central point of contact for all information technology security matters at UL Lafayette. Acting as internal technical consultants, it is this Office's responsibility to create workable information security compromises which take into consideration the needs of Users, Custodians, Stewards, and selected third parties. Reflecting these compromises, this Office defines information security standards, procedures, policies, and other requirements applicable to the entire organization. The IT Security Office is responsible for handling all access control administration activities, monitoring the security of UL Lafayette information systems, and providing information security training and awareness programs to UL Lafayette community. The office is additionally responsible for periodically providing management with reports about the current state of information security at UL Lafayette. While information systems contingency planning is the responsibility of information Custodians, the IT Security Office should nonetheless provide technical consulting assistance related to emergency response procedures and disaster recovery. The IT Security Office is also responsible for organizing a computer emergency response team (CERT) to promptly respond to virus infections, hacker break-ins, system outages, and similar information security problems.

2.8 Internal Audit Department

The UL Lafayette Internal Audit Department periodically performs compliance checks to make sure that the above-mentioned parties are performing their assigned duties, and to make sure that other information security requirements are being consistently observed. Internal Audit acts as the eyes and ears of top management at UL Lafayette, making sure that internal controls (including those related to information security) are consistent with both top management expectations and organizational goals. Any inadequacies in the information security policies shall be brought to the attention of the University IT Security Officer.

2.9 University Operational Review

The University Operational Review is responsible for interpreting the laws that apply to the information security policies and making sure that the policies are consistent with those laws and other University policies. Any inadequacies in the information security policies shall be brought to the attention of the University IT Security Officer who will consult University Counsel and others within the University as appropriate. University Counsel is also responsible for reporting any criminal offense to the appropriate law enforcement agency.

3 Asset Classification

To assist in the appropriate handling of information, a sensitivity classification hierarchy should be used throughout UL Lafayette. This hierarchy provides a shorthand way of referring to sensitivity, and can be used to simplify information security decisions and minimize information security costs. One important intention of a sensitivity classification system is to provide consistent handling of the information, no matter what form it takes, no matter where it goes, and no matter who possesses it. For this reason, it is important to maintain the labels reflecting sensitivity classification categories. UL Lafayette uses three sensitivity classification categories:

3.1 Public Data – (Public Information)

This classification covers information that can be disclosed to any person inside or outside the University. Although security mechanisms are not needed to control disclosure and dissemination, they are still required to protect against unauthorized modification and destruction of information. Examples: marketing brochures and material posted to the UL Lafayette Internet web page. Disclosure of UL Lafayette information to the public requires the existence of this label, the specific permission of the information owner, or long-standing practice of publicly distributing this information.

3.2 Sensitive Data - (Internal Use Only Information)

This classification covers information that requires protection against unauthorized disclosure, modification, destruction, and use, but the sensitivity of the information is less than that for Confidential information. Examples of Internal-use-only information are internal memos, correspondence, and other documents whose distribution is limited as intended by the Stewards.

3.3 Restricted Data - (Confidential Information)

This classification covers sensitive information about individuals, including information identified in the Human Resources Manual, and sensitive information about the University. Information receiving this classification requires a high level of protection against unauthorized disclosure, modification, destruction, and use. Specific categories of confidential information include information about:

- Current and former students (whose education records are protected under the Family Educational Rights and Privacy Act (FERPA) of 1974), including student academic, disciplinary, and financial records (cover under the Gramm-Leach-Bliley Act (GLB)); and prospective students, including information submitted by student applicants to the University.
- Protected Health Information covered under the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
- Research subjects, Law Center clients, library patrons, and donors and potential donors.
- Current, former, and prospective employees, including employment, pay, benefits data, and other personnel information.
- Research, including information related to a forthcoming or pending patent application, and information related to human subjects. Patent applications should be filed within one year of a public disclosure (i.e., an enabling publication or presentation, sale, or dissemination of product reduced to practice, etc.) to preserve United States patent rights. To preserve foreign patent rights, patent applications should be filed prior to public disclosure. Therefore, it is strongly

recommended that prior to any public disclosure, an Invention Disclosure Form be submitted to the Office of Technology Transfer and Business Development for evaluation of the technology and determination of whether to file a patent application, thereby preserving U.S. and foreign patent rights.

- Certain University business operations, finances, legal matters, or other operations of a particularly sensitive nature.
- Information security data, including passwords. Information about security-related incidents.

3.4 Default Classification

Information that is not classified explicitly is classified by default as follows: Information falling into one of the Confidentiality categories listed above is treated as Confidential. Other information is treated as Internal-use-only unless it is published (publicly displayed in any medium) by the Owner, in which case it is classified Public.

4 Administrative Controls

4.1 Security Policies

Policies are the primary embodiment of strategy, guiding decisions made by users, administrators and managers, and informing those individuals of their security responsibilities. Policies also specify the mechanisms through which responsibilities can be met, and provide guidance in acquiring, configuring, and auditing information systems. Key actions that UL Lafayette will follow when developing a security policy are:

- Implementing through ordinary means, such as system administration procedures and acceptable-use policies;
- Enforcing policy through security tools and sanctions;
- Delineating the areas of responsibility for users, administrators, and managers;
- Communicating in a clear, understandable manner to all concerned;
- Obtaining employee certification that they have read and understood the policy;
- Providing flexibility to address changes in the environment; and
- Conducting annually a review and approval by senior management.

4.2 Security Program Management (C-I-A-A)

UL Lafayette establishes and maintains a security program that ensures the availability, integrity and confidentiality of our information resources. Availability, integrity, accountability, and confidentiality are the three basic requirements of security management programs.

4.2.1 Confidentiality

Confidentiality is the protection of information within systems so that unauthorized people, resources, and processes cannot access that information. That is, confidentiality means the system does not allow information to be disclosed to anyone who is not authorized to access it. Privacy issues and regulations such as HIPAA and GLB emphasize the important of confidentiality on protecting personal information and student records maintained in automated information systems.

Confidentiality should be well defined, and procedures for maintaining confidentiality should be carefully implemented. Crucial aspects of confidentiality are **User Identification**, **Authentication** and **Authorization**.

Confidentiality can be compromised in several ways. The following are some of the most common encountered threats to information confidentiality:

- **Hackers**. A hacker is someone who bypasses the system's access controls by taking advantage of security weaknesses that the system's developers have left in the system. In addition, many hackers are adept at discovering the passwords of authorized users who choose passwords that are easy to guess. The activities of hackers represent serious threats to the confidentiality of information in computer systems.
- **Masquerading**. Masquerading is defined as an attempt to gain access to system by posing as an authorized user.

- **Unauthorized user activity**. This type of activity occurs when users gain access to files they are not authorized to access. Weak access controls often enable such compromise confidential information.
- **Unprotected download files**. Downloading can compromise confidential information if, in the process, files are moved from the secure environment of host system to an unsecured PC for local processing. While on the PC, confidential information could be accessed by unauthorized users.
- **Networks.** Networks present a special confidentiality threat because data following through networks can be viewed at any node of the network. This is particularly significant because the unencrypted users IDs and passwords are subject to compromise by a "sniffer". Any confidential information not intended for viewing by everyone should be protected by encryption techniques.
- **Malicious Sofware:** Malicious programs can be programmed to copy confidential files to unprotected area of the system or other resources when they are unknowingly excecute by the users who have authorized to access those files
- **Social engineering**. Social Engineering is a term that describes a no technical kind of intrusion that relies heavily on human interaction and often involves tricking other to break security procedures.

4.2.2 Integrity

Integrity is the protection of systems information or processes from intentional or accidental unauthorized changes. Like confidentiality, integrity can be compromised by hackers, masqueraders, unauthorized user activity, networks, malicious codes because each of these threats can lead to unauthorized change to data or programs. Three basic principles are used to establish integrity controls:

- Granting access on a need-to-know basis
- Separation of duties
- Rotation of duties

4.2.3 Availability

Availability is the assurance that a computer system is accessible by authorized users when needed. Two facets of availability are typically discussed:

- Denial of Service
- Loss of data processing capabilities as a result of nature disasters or human actions.

Denial of Service usually refers to user or intruder actions that tie up the computing services in a way that renders the system unusable by authorized users. Loss of data processing capabilities because of nature disasters or human actions is more common. Such loses are countered by contingency planning which provides an alternative means of processing, therefore ensure availability. Physical, Operations, and Administrative controls are important aspects of security initiatives that addresses availability.

4.2.4 Accountability (Individual Level)

Accountability is the requirement that actions of an entity may be traced uniquely to that entity. Accountability is often an organizational policy requirement and directly supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

4.3 Risk Management

Risk management is an oversight process undertaken on a continuous basis. This process involves risk identification, assessment, control and mitigation. The scope of risk management embraces a broad horizon, which incorporates risk anticipation and preclusion. To quantify risks, it is necessary to assess vulnerabilities, threats, the cost of required security measures, and the impacts of the threats if unmitigated.

UL Lafayette's information security risk management framework should include the following elements:

- Identify the information assets of UL Lafayette.
- Prioritize information assets according to their worth to UL Lafayette.
- Identify, analyze, quantify and mitigate technology risks.
- Implement appropriate security policies and measures to safeguard the integrity and reliability of information assets.
- Protect information assets against external and internal threats.
- Maintain a strong capability to detect and respond to attacks and suspicious activities on its networks or systems.

4.3.1 Risk Management Responsibility

Overall risk management policies are the responsibility of the senior management. Information risks and security threats are not technical issues but business issues. High-level risk management strategy is an oversight process applied on a continuous basis. UL Lafayette should develop risk management processes according to risk acceptance levels, security profiles and the university governance culture. UL Lafayette should also develop rapid response contingency plans in order to be prepared for new risks and new threats, which may arise unexpectedly.

4.4 Assurance

Computer security assurance is the degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes. Assurance is not, however, an absolute guarantee that the measures work as intended. Assurance can be difficult to analyze; however, it is something people expect and obtain (though often without realizing it). For example, people may routinely get product recommendations from colleagues but may not consider such recommendations as providing assurance.

Assurance is a degree of confidence, not a true measure of how secure the system actually is. This

distinction is necessary because it is extremely difficult -- and in many cases virtually impossible -- to know exactly how secure a system is.

Auditing and Monitoring are the two wisely use methods for obtaining assurance.

4.4.1 Auditing

An audit conducted to support assurance examines whether the system is meeting stated or implied security requirements including system and organization policies. Audits can be self-administered or independent (either internal or external). Both types can provide excellent information about technical, procedural, managerial, or other aspects of security. The essential difference between a self-audit and an independent audit is objectivity. Reviews done by system management staff, often called self-audits/ assessments have an inherent conflict of interest. The system management staff may have little incentive to say that the computer system was poorly designed or is sloppily operated. On the other hand, they may be motivated by a strong desire to improve the security of the system. In addition, they are knowledgeable about the system and may be able to find hidden problems

The independent auditor, by contrast, should have no professional stake in the system. Independent audit may be performed by a professional audit staff in accordance with generally accepted auditing standards.

There are many methods and tools, some of which are described here, that can be used to audit a system. Several of them overlap.

Automatic Tools

Automated tools can be used to help find a variety of threats and vulnerabilities, such as improper access controls or access control configurations, weak passwords, lack of integrity of the system software, or not using all relevant software updates and patches. These tools are often very successful at finding vulnerabilities and are sometimes used by hackers to break into systems. Not taking advantage of these tools puts system administrators at a disadvantage. Many of the tools are simple to use; however, some programs (such as access-control auditing tools for large mainframe systems) require specialized skill to use and interpret.

Security Checklists

A checklist should be provided against the system being audited. This list outlines the major security considerations for a system, including management, operational, and technical issues. One advantage of using a computer security plan is that it reflects the unique security environment of the system, rather than a generic list of controls. Other checklists can be developed, which include organizational security policies and practices (often referred to as *baselines*). Lists of "generally accepted security practices" (GSSPs) can also be used. Care needs to be taken so that deviations from the list are not automatically considered wrong, since they may be appropriate for the system's particular environment or technical constraints.

Checklists can also be used to verify that changes to the system have been reviewed from a security point of view. A common audit examines the system's configuration to see if major changes (such as connecting to the Internet) have occurred that have not yet been analyzed from a security point of view.

Penetration Testing

Penetration testing can use many methods to attempt a system break-in. In addition to using active automated tools, penetration testing can be done "manually." The most useful type of penetration testing is to use methods that might really be used against the system. For hosts on the Internet, this would certainly include automated tools. For many systems, lax procedures or a lack of internal

controls on applications are common vulnerabilities that penetration testing can target. Another method is "social engineering," which involves getting users or administrators to divulge information about systems, including their passwords

4.4.2 Monitoring

Security monitoring is an ongoing activity that looks for vulnerabilities and security problems. Many of the methods are similar to those used for audits, but are done more regularly or, for some automated tools, in real time.

Automatic Tools

Several types of automated tools monitor a system for security problems. Some examples follow:

Virus scanners are a popular means of checking for virus infections. These programs test for the presence of viruses in executable program files.

Checksumming presumes that program files should not change between updates. They work by generating a mathematical value based on the contents of a particular file. When the integrity of the file is to be verified, the checksum is generated on the current file and compared with the previously generated value. If the two values are equal, the integrity of the file is verified. Program checksumming can detect viruses, Trojan horses, accidental changes to files caused by hardware failures, and other changes to files. However, they may be subject to covert replacement by a system intruder. Digital signatures can also be used.

Password crackers check passwords against a dictionary (either a "regular" dictionary or a specialized one with easy-to-guess passwords) and also check if passwords are common permutations of the user ID. Examples of special dictionary entries could be the names of regional sports teams and stars; common permutations could be the user ID spelled backwards.

Integrity verification programs can be used by such applications to look for evidence of data tampering, errors, and omissions. Techniques include consistency and reasonableness checks and validation during data entry and processing. These techniques can check data elements, as input or as processed, against expected values or ranges of values; analyze transactions for proper flow, sequencing, and authorization; or examine data elements for expected relationships. These programs comprise a very important set of processes because they can be used to convince people that, if they do what they should not do, accidentally or intentionally, they will be caught. Many of these programs rely upon logging of individual user activities.

Intrusion detectors analyze the system audit trail, especially log-ons, connections, operating system calls, and various command parameters, for activity that could represent unauthorized activity.

System performance monitoring analyzes system performance logs in real time to look for availability problems, including active attacks (such as the 1988 Internet worm) and system and network slowdowns and crashes.

System Logs

a periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours.

Configuration Management

From a security point of view, configuration management provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. Configuration management can be used to help ensure that changes

take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including its security

Changes to the system can have security implications because they may introduce or remove vulnerabilities and because significant changes may require updating the contingency plan, risk analysis, or accreditation.

5 Operations Security

Operation security identified the controls over hardware, media, and the operators and administrators with access privileges to these resources. It is the process of safeguarding information assets when the data is at rest, in processing state or in transmitting state through communication links.

5.1 Personnel Security

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relate to how these individuals interact with computers and the access and authorities they need to do their job. No computer system can be secured without properly addressing these security issues.

Personnel Security refers to those practices, technologies and/or services used to ensure that personnel security safeguards are applied appropriately to those personnel working for, or on behalf, of the University.

UL Lafayette ensures the confidentiality, integrity and availability of its information systems by implementing reasonable safeguards to ensure that all members of its workforce have appropriate access to its information systems, while preventing those workforce members who do not have access from obtaining access to information systems. UL Lafayette will establish the following policies as part of its commitment to complying with this standard:

- UL Lafayette ensures that workforce members who work with or have the ability to access its information systems are properly authorized and/or supervised.
- UL Lafayette's workforce members are screened during the hiring process.
- University implements a documented process for terminating access to its information systems when employment of workforce members ends or when access is no longer appropriate.
- UL Lafayette's workforce members are required to sign an Acceptable Use of Electronic Resource Agreement.

5.2 Business Continuity Management

UL Lafayette should seek to identify the consequences of disasters, security failures and loss of service and should develop contingency plans. Risks should be understood in the terms of their likelihood. Regular testing, documentation and updates are required. Updates are required if there are changes in personnel, addresses or telephone numbers, business strategy, location, legislation and changes in contractors, suppliers and key customers.

5.3 Computer Security Incident Handling

Computer systems are subject to a wide range of mishaps -- from corrupted data files, to viruses, to natural disasters. Some of these mishaps can be fixed through standard operating procedures. For example, frequently occurring events (e.g., a mistakenly deleted file) can usually be readily repaired (e.g., by restoration from the backup file). More severe mishaps, such as outages caused by natural disasters, are normally addressed in an organization's contingency plan. Other damaging events result from *deliberate malicious technical activity* (e.g., the creation of viruses or system hacking).

A computer security incident can result from a computer virus, other malicious code, or a system intruder, either an insider or an outsider. It is used in this section to broadly refer to those incidents

resulting from deliberate malicious technical activity. It can more generally refer to those incidents that, without technically expert response, could result in severe damage.

Although the threats that hackers and malicious code pose to systems and networks are well known, the occurrence of such harmful events remains unpredictable. Security incidents on larger networks (e.g., the Internet), such as break-ins and service disruptions, have harmed various organizations' computing capabilities. When initially confronted with such incidents, most organizations respond in an ad hoc manner. However recurrence of similar incidents often makes it cost-beneficial to develop a standing capability for quick discovery of and response to such events. This is especially true, since incidents can often "spread" when left unchecked thus increasing damage and seriously harming an organization.

Incident handling is closely related to contingency planning as well as support and operations. An incident handling capability may be viewed as a component of contingency planning, because it provides the ability to react quickly and efficiently to disruptions in normal processing. Broadly speaking, contingency planning addresses events with the potential to interrupt system operations. Incident handling can be considered that portion of contingency planning that responds to malicious technical threats.

5.3.1 Computer Incident Response Team (CIRT)

The primary directive of the Computer Incident Response Team is Incident Response Management, which manages UL Lafayette's response to events that pose risk to our computing environment.

The management consists of the following:

- Coordinating the notification and distribution of information pertaining to the incident to the appropriate parties (those with a need to know) through a predefined escalation path.
- Mitigation risk to UL Lafayette Computing Services by minimizing the disruptions to normal business activities and the costs associated with remediating the incident (including public relations)
- Assembling teams of security technical analysts and forensic team to investigate the potential vulnerabilities and to resolve specific intrusions.
- Management of network logs, including collection, retention, review, and analysis pf data
- Management of the resolution of an incident, management of the remediation of a vulnerability, and post-event reporting to the appropriate parties.

5.3.2 Computer Incident Response and Public Relations

UL Lafayette will include in the incident response procedures a predetermined action plan to address public relations issues. Being able to maintain constituent's confidence during a period of crisis or emergency is vital to the university's reputation and survivability.

5.4 Security Considerations in Computer Support and Operations

Computer support and operations refers to everything done to run a computer system. This includes both system administration and tasks external to the system that support its operation (e.g., maintaining documentation). It does not include system planning or design. The support and operation of any computer system, from a three-person local area network to a campus-wide application serving thousands of users, is critical to maintaining the security of a system. Support and operations are routine activities that enable computer systems to function correctly. These include fixing software or

hardware problems, loading and maintaining software, and helping users resolve problems.

The important security considerations within some of the major categories of support and operations are:	➢ **user support** ➢ **software support** ➢ **configuration management** ➢ **backups** ➢ **media controls** ➢ **documentation** ➢ **maintenance**

This section addresses the support and operations activities directly related to security. Every control discussed in this document relies, in one way or another, on computer system support and operations.

5.4.1 User Support

An important security consideration for user support personnel is being able to recognize which problems (brought to their attention by users) are security-related. For example, users' inability to log onto a computer system may result from the disabling of their accounts due to too many failed access attempts. This could indicate the presence of hackers trying to guess users' passwords.

In general, system support and operations staff need to be able to identify security problems, respond appropriately, and inform appropriate individuals. A wide range of possible security problems exist. Some will be internal to custom applications, while others apply to off-the-shelf products. Additionally, problems can be software- or hardware-based.

The more responsive and knowledgeable system support and operation staff personnel are, the less user support will be provided informally. The support other users provide is important, but they may not be aware of the "whole picture."

5.4.2 Software Support

Software is the heart of our computer operations. Therefore, it is essential that software function correctly and be protected from corruption. There are many elements of software support.

One is *controlling what software is used on a system*. If users or systems personnel can load and execute any software on a system, the system is more vulnerable to viruses, to unexpected software interactions, and to software that may subvert or bypass security controls. One method of controlling software is to inspect or test software before it is loaded. This can apply to new software packages, to upgrades, to off-the-shelf products, or to custom software, as deemed appropriate. In addition to controlling the loading and execution of new software, we should also give care to the configuration and use of powerful system utilities. System utilities can compromise the integrity of operating systems and logical access controls

A second element in software support can be to ensure that *software has not been modified without proper authorization*. This involves the protection of software and backup copies. This can be done with a combination of logical and physical access controls.

5.4.3 Backups

Support and operations personnel and sometimes users back up software and data. This function is critical to contingency planning. Frequency of backups will depend upon how often data changes and how important those changes are. Program managers should be consulted to determine what backup schedule is appropriate. Also, as a safety measure, it is useful to test that backup copies are actually usable. Finally, backups should be stored securely, as appropriate.

5.4.4 Media Controls

Media controls include a variety of measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media. From a security perspective, media controls should be designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, when stored outside the system. This can include storage of information before it is input to the system and after it is output.

Media Labeling

Controlling media may require some form of physical labeling. The labels can be used to identify media with special handling instructions, to locate needed information, or to log media (e.g., with serial/control numbers or bar codes) to support accountability. Identification is often by colored labels on diskettes or tapes or banner pages on printouts.

Media Logging

The logging of media is used to support accountability. Logs can include control numbers (or other tracking data), the times and dates of transfers, names and signatures of individuals involved, and other relevant information. Periodic spot checks or audits may be conducted to determine that no controlled items have been lost and that all are in the custody of individuals named in control logs. Automated media tracking systems may be helpful for maintaining inventories of tape and disk libraries.

Media Transmittal

Media control may be transferred both within the organization and to outside elements. Possibilities for securing such transmittal include sealed and marked envelopes, authorized messenger or courier, or U.S. certified or registered mail.

Media Disposition

When media is disposed of, it may be important to ensure that information is not improperly disclosed. This applies both to media that is *external* to a computer system (such as a diskette) and to media *inside* a computer system, such as a hard disk. The process of removing information from media is called *sanitization*.

Three techniques are commonly used for media sanitization: overwriting, degaussing, and destruction. *Overwriting* is an effective method for clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination) onto the media. Common practice is to overwrite the media three times. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a *delete* command is used). Overwriting requires that the media be in working order. *Degaussing* is a method to magnetically erase data from magnetic media. Two types of degausser exist: strong permanent magnets and electric degaussers. The final method of sanitization is destruction of the media by shredding or burning.

5.4.5 Documentation

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

The security of a system also needs to be documented. This includes many types of documentation, such as security plans, contingency plans, risk analyses, and security policies and procedures. Much of this information, particularly risk and threat analyses, has to be protected against unauthorized disclosure. Security documentation also needs to be both current and accessible. Accessibility should take special factors into account (such as the need to find the contingency plan during a disaster).

Security documentation should be designed to fulfill the needs of the different types of people who use it. For this reason, many organizations separate documentation into *policy* and *procedures*. A *security procedures manual* should be written to inform various system users how to do their jobs securely. A security procedures manual for systems operations and support staff may address a wide variety of technical and operational concerns in considerable detail.

5.4.6 Maintenance Account

System maintenance requires either physical or logical access to the system. Support and operations staff, hardware or software vendors, or third-party service providers may maintain a system. Maintenance may be performed on site, or it may be necessary to move equipment to a repair site. Maintenance may also be performed remotely via communications connections. If someone who does not normally have access to the system performs maintenance, then a security vulnerability is introduced.

In some circumstances, it may be necessary to take additional precautions, such as conducting background investigations of service personnel. Supervision of maintenance personnel may prevent some problems, such as "snooping around" the physical area. However, once someone has access to the system, it is very difficult for supervision to prevent damage done through the maintenance process.

Many computer systems provide *maintenance accounts*. These special log-in accounts are normally preconfigured at the factory with pre-set, widely known passwords. *It is critical to change these passwords or otherwise disable the accounts until they are needed.* Procedures should be developed to ensure that only authorized maintenance personnel can use these accounts. If the account is to be used remotely, authentication of the maintenance provider can be performed using call-back confirmation. This helps ensure that remote diagnostic activities actually originate from an established phone number at the vendor's site. Other techniques can also help, including encryption and decryption of diagnostic communications; strong identification and authentication techniques, such as tokens; and remote disconnect verification.

Larger systems may have *diagnostic ports*. In addition, manufacturers of larger systems and third-party providers may offer more diagnostic and support services. It is critical to ensure that these ports are only used by authorized personnel and cannot be accessed by hackers.

5.5 Physical and Environmental Security

Physical and Environmental Security refer to those practices, technologies and/or services used to ensure that physical security safeguards are applied. Physical security safeguards take into account 1) the physical facility housing the information resources; 2) the general operating location; and 3) the support facilities that underpin the operation of the information systems.

Physical security safeguards provide a first line of defense for information resources against physical damage, physical theft, unauthorized disclosure of information, loss of control over system integrity, and interruption to computer services.

UL Lafayette limits physical access to information resources and the facilities in which they are located while taking reasonable steps to ensure that properly authorized workforce members have access to such information resources and facilities. UL Lafayette ensures, where possible, that information resources are located in areas where physical access can be controlled in order to minimize the risk of unauthorized access. UL Lafayette takes reasonable steps to ensure that the level of protection provided for the information resources, as well as the facilities in which they are housed, is commensurate with that of the identified threats and risks. UL Lafayette will establish the following policies and procedures as part of its commitment to complying with this standard:

- Mission critical system facilities should be located in a secure location that is locked and restricted to authorized personnel only.
- Access to "critical" computer hardware, wiring, displays and networks should be controlled by rules of least privilege.
- System configurations (i.e., hardware, wiring, displays, networks) of "critical" systems should be documented. Installations and changes to those physical configurations should be governed by a formal change management process.
- A system of monitoring and auditing physical access to "critical" computer hardware, wiring, displays and networks should be implemented (e.g. badges, cameras, access logs).

5.6 Change Control Management

Change control management is the key ingredient that authorized changes to production system, including system and application software. Changes to production system include the implementation of new applications, modification of existing applications, removing old applications or upgrading, patching system software. From security viewpoint, we are concerned with potential security impact of these changes, especially if they are not documented or approved by management.

Historically, the most easily sidestepped control is change control. Therefore, we should have a policy regarding changes to operation systems, computing equipment, networks, and applications. A policy is needed for change to be effective and orderly.

Change management procedures should be designed to ensure that the costs and benefits of change are properly analyzed and that changes to systems are mode in a controlled way. An outline of Change Management Process is:

- A change is requested by completion of a change request form.
- A change request form is analyzed for validity.
- The ways the change could be implemented are analyzed.
- The costs associated with the change are analyzed.
- The analysis and change recommendations are recorded.
- The change request is given to change control board for final decision.
- Accepted changes are made and recorded.
- The change implementation is submitted to quality control for approval.

During this process, the IT Security Office or his designee should have an opportunity to review the changes to ensure that changes do not result in bypass or erosion of the required security control. Thus, it is important for the ITSO to be involved in change review at the earliest point in the process.

5.7 Protection and Control Against Malicious Software

As part of defense-in-depth strategy, UL Lafayette deploys malicious software checking programs at the firewall, perimeter (edge) of the network and on individual end-user systems. Anti-virus software is installed on all Systems and workforce members are prohibited from bypassing or disabling such software unless properly authorized to do so. As described in the E-mail Security Section, antivirus software examines all electronic mail attachments, downloads, and electronic media to confirm they do not contain malicious software. UL Lafayette subscribes to updates for all malicious software checking programs, including anti-virus software.

5.8 Email Security and Control

E-mail is an essential element of business today, providing convenient, time-saving communication with co-workers, students and collaborators. Anything that threatens the integrity, reliability and performance of e-mail has a profound impact on business operations. Spam is currently the biggest e-mail threat, and UL Lafayette should take action to protect our e-mail systems.

5.8.1 Spam Control

With the volume and threat of spam on the rise, the business costs of spam have increased dramatically. The sheer volume of spam pouring into UL Lafayette e-mail systems has required us to increase the capacity of our e-mail systems with costly network and infrastructure investments to keep pace. An August 2003 study from the Radicati Group reported that spam forces enterprises to spend an average of $49 per email user per year to handle the load.

Spam drains employee productivity as workers waste time reading, deleting or even responding to spam e-mails. Additionally, the sexually explicit nature of many spam messages poses potential liability for UL Lafayette.

Although it takes a person only a moment to process a message and identify it as spam, it is difficult to automate that human process because no single message characteristic consistently identifies spam. In fact, there are hundreds of different message characteristics that may indicate an e-mail is spam, and an effective anti-spam solution should be capable of employing multiple spam detection techniques.

In addition to effectively identifying spam, UL Lafayette should be assured legitimate mail is not blocked in error. Even one false positive, or incorrectly blocked e-mail, can have a significant impact on businesses today. Accurate spam blocking requires a combination of tools to examine various message criteria combined with real-time research and intelligence data.

By aggregating multiple spam detection technologies, UL Lafayette can combine the benefits of each individual technique while minimizing the drawbacks.

5.8.2 Virus Control

The widespread adoption of email through the years has been accompanied by the development of malicious code, that is, email viruses and attacks. Email has provided hackers and crackers with an easy way to distribute harmful content to the internal network. Campus LANs have been breached by worms and viruses, as well as by crackers, through the use of email. Hackers can easily circumvent the

protection offered by a firewall by tunneling through the email protocol. A typical firewall cannot protect against such email attacks, because it simply does not analyze email and its contents.

Because email messages can include file attachments, hackers can send infected files and hope that the recipient will open them, as happened with Melissa and Manwella. This method makes use of social engineering to urge the end user to run the file. Yet, other methods exist which allow a skilled and possibly malevolent cracker to inject code through email and run custom-made applications automatically while the end user reads the email text. Such problems have been around since the use of HTML in email and have been exploited by notorious worms such as the KaK worm, BubbleBoy virus or the more recent Nimda.

Although anti-virus products can catch many viruses and worms, hackers are able to dodge such protection by producing their own customized code. This can result in dangerous threats penetrating the campus network through lesser known methods and through bypassing anti-virus protection and other traditional anti-hacker protection. The threat posed by hackers to the internal network is huge, as internal network security is low to ensure usability.

To control the spread of email virus, UL Lafayette needs to protect against the methods described above through content filtering, attachment checking and virus scanning of all incoming and outgoing emails at Exchange Server and SMTP gateway level. Furthermore, it is desirable to adopt the use of multiple virus engines in multiple locations, for better protection.

5.8.3 Privacy Control

In addition to the usual concerns about privacy and security of e-mail correspondence, UL Lafayette should now consider the regulatory compliance requirements associated with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Administrative Simplification section of HIPAA Security Rule mandates privacy and security of electronic Protected Health Information (e-PHI). HIPAA, as it relates to e-mail security, is an enforcement of otherwise well-known best practices that include:

- Ensuring that e-mail messages containing confidential information are kept secure when transmitted over an unprotected link
- Ensuring that e-mail systems and users are properly authenticated so that confidential information does not get into the wrong hands
- Protecting e-mail servers and message stores where confidential information may be stored

As covered entities under HIPAA, UL Lafayette should comply and put these practices in place.

5.9 Intrusion Prevention/Detection Systems

The evolution of hybrid computer attacks utilizing multiple vectors to breech security infrastructure has highlighted the need for enterprises to defend themselves against a constantly shifting threat.

Organizations have suffered catastrophic damage to their business confidentiality, integrity, and availability as intrusions have become more virulent. In a matter of minutes, companies can suffer significant lost revenue as production lines go dark and order taking and fulfillment processes come to a halt due to attacks like Sasser, SQL Slammer, and Nimda.

Traditional firewall and anti-virus solutions are necessary to prevent the transfer of malicious code, but are not sufficient to address the new generation of threats and targeted attacks. Security solutions that proactively protect vital information assets in real time, without waiting for new signature creation and

distribution, are needed.

In the recent report titled Intrusion Prevention by the Department of Trade and Industry (DTI), it was concluded that the time and resources spent on investigation and remediation are remarkably high for such attacks and intrusions. Such costs will be significantly reduced with an Intrusion Prevention System (IPS), since an IPS solution will provide a proactive measure of protection.

Due to the dynamic nature of network intrusions and threats, deploying a combination of both network and host IPS technologies provides the greatest level of protection for critical data and critical applications. Network IPS solutions are deployed inline at the network perimeter, core, or remote office. They are designed to protect UL Lafayette critical infrastructure by blocking internal and external attacks on the wire and are considered the first line of defense. Host IPS solutions are deployed on servers, desktops, and laptops. They are designed to protect critical systems and applications by blocking attacks at the host and are considered the last line of defense.

6 Technical Controls

6.1 Identification and Authentication (I&A)

I&A is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability. Access control often requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses required to perform their duties. User accountability requires the linking of activities on a computer system to specific individuals and, therefore, requires the system to identify users.

Identification is the means by which a user *provides* a claimed identity to the system. *Authentication* is the means of establishing the *validity* of this claim.

There are three means of authenticating a user's identity, which can be used alone or in combination:

- something the individual *knows* (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key);
- something the individual *possesses* (a token -- e.g., an ATM card or a smart card); and
- something the individual *is* (a biometric -- e.g., such characteristics as a voice pattern, handwriting dynamics, or a fingerprint).

UL Lafayette is currently implementing I&A with a user ID or user Social Security Number coupled with something the user knows (password) for all systems. However, because of privacy issue UL Lafayette will discontinue the use of the social security number as the user identifier and moving forward with a Campus-Wide ID described below.

The security of a password system is dependent upon keeping passwords secret. Unfortunately, there are many ways that the secret may be divulged. This problem can be significantly mitigated by improving password security, as discussed in the Password Management Section.

6.1.1 Campus-Login Identification (CLID)

In an effort to increase the level of protection given to Social Security numbers, UL Lafayette is moving forward with a Campus-Login ID (CLID). This change will eventually allow students to use services and identify themselves to individuals inside and outside of the University without ever revealing their social security number (SSN).

It should be recognized that UL Lafayette can never totally eliminate the need for Social Security numbers. They are still required for a number of purposes including processing federal aid, reporting income of student workers, or obtaining official transcripts. However, the use of Social Security numbers will be significantly reduced with the use of the Campus-Login Identification numbers.

6.1.2 Password Management

The password is a protected word that authenticates the user to the system. The theory is that a user has a secret password, something only the user knows; and when the password is entered into the system, it should be the user, because the user is the only one who knows the secrete password.

The problem with this theory is the secrecy of password. Users might right it down, tape it to the monitor or underneath the keyboard, share it with others, or make it so simple that it is easily guessed.

Because of the ease in compromising reusable passwords, they are not considered adequate control by themselves.

A passphrase is a sequence of characters or words used as an alternative to a password. There is no real difference between the two, except in the meaning of the terms themselves: "password" encourages users to think short and easy, whereas "passphrase" is meant to encourage the user to type in a complete phrase.

Recommendations for implementation and management of passwords or passphrases are:

- Password lifetime should be restricted.
- Users should create passwords that are not dictionary words for names.
- Users should create passwords using a mix of alphabetic, numeric, and special characters.
- Users should create longer passwords, which tend to be more secure.
- Many operating systems can be configured to lock a user ID after a set number of failed login attempts. This helps to prevent guessing of passwords.

Creating a good passphrase is one of the most important things that can be done to preserve the privacy of computer data and email messages. A passphrase should be:

- Known only to the creator
- Long enough to be secure
- Hard to guess, even by someone who knows the user well
- Easy to remember and easy to type accurately.

Because passwords are a vital element of access control in our environment, it is important to protect access to the password file. Typically, passwords are stored in a password database file that uses on-way hash algorithm. Therefore, the hash algorithm should be protected. For security measures, the operating system should offer both encryption and other access control to protect the password file.

6.2 Access Controls

Access controls are collection of mechanisms that specify what users can do on the system or network such as what resources they can access and what operations they can perform. They are countermeasures for ensuring that only users with proper need and authority can access the system or network, are allowed to use network services or execute programs, can read, edit, add and delete the appropriate information on the system.

Access controls are implemented to ensure the availability, integrity, and confidentiality of information and information systems. Separation of duties and least privilege are the two of standards of access control.

6.2.1 Segregation of Duties

The segregation of duties avoids the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner and in the normal course of business processes. Segregation of duties is an important means by which fraudulent and or malicious acts can be discouraged and prevented.

When duties are segregated, access to the computer, the production data library, the production programs, the programming documentation and the operating system and associated utilities can be

limited. Potential damage from the actions of any one person is therefore reduced. The Technology Services and end-user departments should be organized to achieve an adequate segregation of duties.

The segregation of duties control matrix below is not an industry standard, but guideline indicating which positions should be separated and which require compensating controls when combined. The matrix is illustrative of potential segregation of duties issues and should not be viewed or used as an absolute, rather it should be used to help identify potential conflicts so proper questions may be asked to identify compensating controls.

6.2.2 Least Privilege

Least privilege is a policy that limits both the system's users and processes to access only those resources necessary to perform assigned functions. Ensuring least privilege requires identifying what each user's job is, outlining the minimum set of privileges required to perform that job, and restricting the user to only those privileges on the system/network. Users only get access to those resources necessary to do their job – no more no less. By restricting access to only those privileges necessary for performing job duties, access is denied to privileges that might be used to circumvent security.

6.2.3 Logical Access Control

Access is the ability to do something with a computer or network resource. *Access control* is the means by which the ability is explicitly enabled or restricted in some way. Computer-based access controls are called *logical access controls*. Logical access controls can prescribe not only who or what (e.g., in the case of a process) is to have access to a specific system resource but also the type of access that is permitted. These controls may be built into the operating system, may be incorporated into applications programs or major utilities (e.g., database management systems or communications systems), or may be implemented through add-on security packages. Logical access controls may be implemented internally to the computer system being protected or may be implemented in external devices.

6.2.4 Network Access Control

A key principle underpinning a high standard of IT Security is that access to computer network resources should be authorized on a 'need to use' basis. Currently, most computers can connect to the University wire/wireless network without authentication and have full access to almost every other computer on the University network. The risk of compromise to UL Lafayette computers can be reduced significantly without affecting normal use if the machines/users are authenticated and segregated on the network according to their usage requirements.

The purpose of the Network Access Control is to define a set of computer connection classes, designed to minimize the exposure to UL Lafayette from destruction, theft and loss of data (eg. confidentiality and privacy), disruption to business operations, and damage to the University's image, which may follow from unauthorized use of its electronic resources.

The Network Access Control defines the roles of Faculty, Staff and ResNET (student) computers when connected to the University's network and defines permissible communications flows between them.

6.2.5 External Access Control: Firewall and DMZ

Firewalls block or filter access between two networks, often between a private network and a larger, more public network such as the Internet, which attract malicious hackers. Firewalls allow internal users to connect to external networks and at the same time prevent malicious hackers from compromising the internal systems.

In addition to reducing the risks from malicious hackers, firewalls have several other benefits. They can reduce internal system security overhead, since they allow an organization to concentrate security efforts on a limited number of machines. (This is similar to putting a guard on the first floor of a building instead of needing a guard on every floor.)

A second benefit is the centralization of services. A firewall can be used to provide a central management point for various services, such as advanced authentication, e-mail, or public dissemination of information. Having a central management point can reduce system overhead and improve service.

6.2.6 Remote Access Control

The decentralized an increasingly mobile workforce place new demand on remote access to the University network. College recruiters, Executives, Faculties, staffs and road warriors all want high speed and reliable and secure access to their data, email and applications.

Remote access technologies consist of any technology and application that allow user access to the campus network when he does not have a physical LAN connection. Remote access can consist of modem or VPN through an internet service provider

Regardless of how complex the network and how the remote access services are acquired, the following security elements are considered:

- **Authentication:** verify the user's login credentials and allow only those who have authorization access to the network.
- **Access Restriction:** to define the resources the user can access.
- **Time Restriction:** restricting when a user can connect and for what duration of time the connection is allowed.
- **Connection Restriction:** impose limit of simultaneous connections per user, consecutive failed attempts, and users of use.
- **Protocol Restriction:** restrict what protocols and services are available through the dial-up
- **Data Encryption:** Protect communication links from eavesdroppers to preserve the integrity and confidentiality of transmitted data.

In addition, remote access users are required to have personal firewalls and anti-virus software on their desktops to prevent another system from accessing them while connected to the remove access service.

6.3 Security Awareness and Education

People, who are all fallible, are usually recognized as one of the weakest links in securing systems. The purpose of computer security awareness, training, and education is to enhance security by:

- improving awareness of the need to protect system resources
- developing skills and knowledge so computer users can perform their jobs more securely
- building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Making computer system users aware of their security responsibilities and teaching them correct practices helps users change their behavior. It also supports *individual accountability*, which is one of the most important ways to improve computer security. Without knowing the necessary security

measures (and to how to use them), users cannot be truly accountable for their actions.

6.4 Software Development and Maintenance

The security of data and information is one of the most important elements of information system security. Through hardware and software mechanism, we process and access data on the system. Thus, it is important to prevent unauthorized access and to protect the system from harm. The objectives to make sure that the system and its resources are **available** when needed, that the **integrity** of the processing of data and the data itself is ensured, and that the **confidentiality** of the data is protected.

Application development procedures are vital to the integrity of systems. If applications are not developed properly, data may be processed in such a way that the integrity of the data is corrupted. In addition, the integrity of the application software itself should be maintained, both in term of change control and terms of attack from malicious software. In addition, if confidentiality is required for data, encryption mechanism should be built into the programming code from the beginning, and not added on as an afterthought.

6.4.1 Incorporation of Security into Software Development Life Cycle (SDLC)

The software development life cycle, or SDLC, encompasses all of the steps that an organization follows when it develops software tools or applications. Organizations that incorporate security in the SDLC benefit from products and applications that are secure by design. Those that fail to involve information security in the life cycle pay the price in the form of costly and disruptive events.

A typical SDLC model contains the following main functions:

- Conceptual definition: This is a basic description of the new product or program being developed, so that anyone reading it can understand the proposed project.
- Functional requirements and specifications: This is a list of requirements and specifications from a business function perspective.
- Technical requirements and specifications: This is a detailed description of technical requirements and specifications in technical terms.
- Design: This is where the formal detailed design of the product or program is developed.
- Coding: The actual development of software.
- Test: This is the formal testing phase.
- Implementation: This is where the software or product is installed in production

For all application systems, security should be considered by systems designers and developers from the beginning of the systems design process through conversion to a production system. While consideration early in the development process is desirable because it is considerably more efficient and effective, this should not be the end of the control selection process. Typically the software development life cycle will involve several points where security is formally included in the process. Hand-rendered signatures (or perhaps digital signatures) indicating the adequacy of security work may be required at these points. The intention here is to require the technical staff to consider security as a formal part of the software development life cycle.

6.4.2 Data Validation

Input data validation should include checks for out-of-range values, invalid characters in data fields, missing or incomplete data, the exceeding of upper and lower data volume limits, unauthorized or

inconsistent control data, and the procedures for responding to these issues. Data balances should be validated, and data should be validated within the program.

The integrity of data and software should be checked. Message authentication should be performed.

6.4.3 Production System Definition

Information systems which have been designated "production systems" have special security requirements. A production system is a system which is regularly used to process information critical to UL Lafayette's business. Although a production system may be physically situated anywhere, the production system designation is assigned by the Technology Services Director of Systems and Operation.

6.4.4 Special Production System Requirements:

Production systems should also have designated Stewards and Custodians for the critical information they process. The IT Security Office should perform periodic risk assessments of production systems to determine whether the controls employed are adequate. All production systems should have an access control system to restrict who can access the system as well as restrict the privileges available to these Users. A designated access control administrator (who is not a regular User on the system in question) should be assigned for all production systems.

6.4.5 Separation Between Production, Development, and Test Systems

Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is maintained in a much more rigorous way for the production system, while the other two environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff should not be permitted to have access to production systems. Likewise, all production software testing should proceed with sanitized information (where Confidential or Highly Restricted information is replaced with dummy data). All security fixes provided by software vendors should also go through the SDM testing process, and should be promptly installed. On a related note, application programmers should not be given access to production information. A formal and documented change control process should also be used to restrict and approve changes to production systems. All application-program-based access paths other than the formal User access paths should be deleted or disabled before software is moved into production.

6.4.6 User Programming

Users are not permitted to write production computer programs unless specifically authorized by the Chief Information Officer. The construction of spreadsheet formulas, automatic execution scripts which are run when a system is booted, or databases is not considered programming for purposes of this document. Both Users and Programmers should be careful never to embed user-IDs or readable passwords in any file.

6.5 Audit Trails

Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.

Audit trails may be used as either a support for regular system operations or a kind of insurance policy or as both of these. As insurance, audit trails are maintained but are not used unless needed, such as

after a system outage. As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems.

Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis.

6.6 Cryptography

Cryptography is used to protect data *both* inside and outside the boundaries of a computer system. Outside the computer system, cryptography is sometimes the *only* way to protect data. While in a computer system, data is normally protected with logical and physical access controls (perhaps supplemented by cryptography). However, when in transit across communications lines or resident on someone else's computer, data cannot be protected by the originator's logical or physical access controls. Cryptography provides a solution by protecting data even when the data is no longer in the control of the originator

6.6.1 Data Encryption

One of the best ways to obtain cost-effective data confidentiality is through the use of encryption. Encryption transforms intelligible data, called *plaintext*, into an unintelligible form, called *ciphertext*. This process is reversed through the process of decryption. Once data is encrypted, the ciphertext does not have to be protected against disclosure. However, if ciphertext is modified, it will not decrypt correctly.

Both secret key and public key cryptography can be used for data encryption although not all public key algorithms provide for data encryption.

To use a secret key algorithm, data is encrypted using a key. The same key should be used to decrypt the data.

When public key cryptography is used for encryption, any party may use any other party's public key to encrypt a message; however, only the party with the corresponding private key can decrypt, and thus read, the message.

Since secret key encryption is typically much faster, it is normally used for encrypting larger amounts of data.

6.6.2 User Authentication

Cryptography can increase security in user authentication techniques. Cryptography is the basis for several advanced authentication methods. Instead of communicating passwords over an open network, authentication can be performed by demonstrating knowledge of a cryptographic key. Using these methods, a one-time password, which is not susceptible to eavesdropping, can be used. User authentication can use either secret or public key cryptography.

7 HIGH-LEVEL SECURITY PRACTICES

UL Lafayette will implement the following security practices. Implementing these practices does not preclude implementation of other security practices or procedures.

1. **Deploy Secure Operating Systems.** Systems software and firewalls will be configured to the highest security settings consistent with the level of protection required, keeping abreast of enhancements, updates and patches recommended by system vendors.
2. **Change Default Passwords.** Default passwords for new systems will be changed immediately upon installation as they provide the most common means for intruders to break into systems.
3. **Install firewalls.** Firewalls will be installed between internal and external networks as well as between geographically separate sites.
4. **Design Redundancies**. Develop built-in redundancies for single points of failure which can bring down the entire network.
5. **Engage independent security specialists**. Independent security specialists will be engaged to assess the strengths and weaknesses of internet-based applications, systems and networks before each initial implementation, and at least annually thereafter, preferably without forewarning to internal staff.
6. Conduct penetration testing at least annually.
7. Use network scanners, intrusion detectors and security alerts.
8. Implement anti-virus software and apply updates regularly.
9. Establish network surveillance and security monitoring procedures.
10. Conduct regular system and data integrity checks.
11. Maintain access security logs and audit trails.
12. Analyze security logs for suspicious traffic and intrusion attempts.
13. Establish an incident management and response plan.
14. Test the predetermined action plan relating to security incidents.
15. Install network analyzers which can assist in determining the nature of an attack and help in containing such an attack.
16. Develop and maintain a recovery strategy and business continuity plan based on total information technology, operational and business needs.
17. Maintain a rapid recovery capability.
18. Conduct security awareness education and programs.
19. Require frequent audits to be conducted by security professionals or internal auditors who have the requisite skills.
20. Separate physical/logical environments for systems development, testing and production.
21. Provide separate environments for the development, testing, staging and production of internet facing web-based applications; connect only the production environment to the internet.
22. Implement a multi-tier application architecture which differentiates session control, presentation logic, server side input validation, business logic and database access.
23. *Turn on WPA2 256-bit encryption in wireless local area networks and install additional user authentication with encryption enhancements.*

8 References

1. British Standard Institute: “ISO 27002 - The Information Security Standard.”
2. IT Governance Institute: “Control Objective for Information and related Technology (CoBIT) Security Control Baseline.”
3. UL Lafayette (2011). “HIPAA Information Security Strategy for HIPAA”
4. National Institute of Standards and Technology Computer Security Resource Center. “Publication 800-12: An Introduction to Computer Security.”
5. Information Systems Audit and Control Association (2005). “CISA Review Manual 2005.”
6. Information Systems Audit and Control Association (2005). “CISM Review Manual 2005.”
7. Cyber Security Task Force Report, (2004). “Improving Security Across the Software Development Life Cycle”
8. International Information Systems Security Certification Consortium (ISC)^2. “Official Guide to CISSP Exam”
9. Wood C (2002). “Information Security Policies Made Easy 8th Edition.”
10. Tipton H, Krause M (2000). “Information Security Management Handbook 4th Edition.”
11. Kovacich G, (2003). “Information Systems Security Officer’s Guide 2nd Edition.”