LAKE-SUMTER STATE COLLEGE
ADMINISTRATIVE PROCEDURE

TITLE: INFORMATION SYSTEMS RESOURCES NUMBER: PRO 7-06

REFERENCE: Board Rule 2.16

I. GENERAL INFORMATION

a. LSSC information Technology Systems are designed for approved present and future users. Users are defined but not limited to LSSC full-time and part-time employees, LSSC students, students from other educational facilities, members of the community, and others as defined by contractual agreements. These resources are administered by the Information Technology Department and are intended for the legitimate business use of the college.

b. Accounts on LSSC's servers are provided for individual users and are not transferable. The person for whom an account has been created is responsible for use of that account. Account holders are encouraged to develop uses which meet their individual needs and which take advantage of the network's functions, including communication systems, Web resources and data resources.

c. The LSSC Information Technology resources, which include telecommunication resources, are expected to be used in a responsible, efficient, ethical and legal manner that support learning and teaching in accordance with the mission of LSSC. Such material must not contain sexually explicit images, messages, or cartoons; or ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based upon their race, national origin, color, sex, sexual orientation, age, disability, or religious or political beliefs. These prohibitions do not apply to material required for College business or legitimate academic purposes. The communication system must not be used to convey any materials that are political, slanderous or controversial.

d. Using the LSSC Information Technology Systems resources to copy or otherwise transmit any content that is unlawful, in violation of patents, trademarks, trade secrets, copyright law, license agreements, and protected material as defined by Florida Statute and Federal law is strictly prohibited.

e. All information and data recorded on electronic media are public records and as such are subject to access by the general public as well as the press in the same manner as physical documents. Thus, any electronic communication concerning any official business may be deleted or destroyed only in accordance with State of Florida Basics of Records Management. Such material can always be retrieved, and may be reviewed at any time by the College to ensure compliance with Rule 2.16 (Information Technology Resources) and this procedure, and may also be reviewed by the public upon a proper request under the Florida Sunshine Law.

f. To ensure that the use of the College Information Technology Systems and other electronic communications systems are consistent with the College's legitimate business interests and not in violation of Rule 2.16 (Information Technology Resources), authorized representatives of the College will monitor the use of such equipment from time to time. Such monitoring will be implemented to support identification, termination, and prosecution of unauthorized activity. The monitoring may include, but will not be limited to, reviewing potential phishing emails, ransomware attacks, malware and viruses; recording access to the system, file transfers, terminal connections, sent and received e-mail messages and voicemail messages, websites visited, phone use, software installation for licensing purposes, and the date, time, and user associated with such events.

II. OWNERSHIP AND USE

a. All IT Systems resources, including hardware, software and telecommunication purchased for supporting learning, teaching, and other work associated with the operation of LSSC, are the property of the College unless specifically stipulated otherwise in the grant, in a joint-use agreement, or by the donor. Department and Program personnel and custodians of the IT Systems resources purchased for their areas and are responsible for the proper care, operation, and use of resources. As custodians only, employees may not take IT Systems resources with them if and when they leave the employment of the College.

b. Access is granted to IT Systems resources, including computer labs, online resources, and communication resources, subject to availability and authorization by the appropriate LSSC authority.

c. If IT Systems resources are purchased under the auspices of grants or other external funding those resources must be used for the intent for which they were purchased, in accordance with the guidelines of the external funding agent, at least until such time as the grant-funded program ends. Once the grant-funded program ended, the IT Systems resources should continue to be used for the original intent for which they were purchased unless the original purpose no longer exists, in which case the resources maybe diverted to other-college-related users.

III. EMPLOYEES

Employees are issued authorization for specific codes and access to carry out Assigned responsibilities. Authorization for expanded or additional access to stored information beyond any regular assigned codes and files requires approval of the individual's supervisor and the Chief Information Officer.

IV. STUDENTS

a. It is recognized that educational institutions play a unique role in promoting intellectual freedom. They serve as a point of voluntary access to information and ideas and as a learning laboratory for students as they develop critical thinking and problem-solving skills needed in a pluralistic society. Acceptable use of IT Systems resources includes supporting instructional, cultural, social, and community service programs of the College. Therefore, LSSC students are allowed access to Internet resources with the understanding that some material that can be accessed is inaccurate or may contain elements that may not meet community or personal standards of decency. The College shall not be held accountable for the accuracy or decency of data retrieved via the Internet.

b. The LSSC IT department employs various measures to protect the security of its system's resources and its users' accounts. Students should be aware, however, that the IT department cannot guarantee security and confidentiality. The College accepts no responsibility for harm caused directly or indirectly by the use of IS resources.

c. All equipment provided for student use belongs to LSSC. The IT department may monitor software installations for licensing purposes on each PC, and monitor hardware for inventory and possible pre-failure diagnostics. Students enrolled in online classes at LSSC are responsible for maintaining their own computers and Internet access. LSSC cannot provide repair or technical assistance for students' equipment and does not act as an ISP (Internet Service Provider).

V. GENERAL PUBLIC

a. Use of the College's IT Systems is primarily restricted to students, faculty and staff. Computers in classrooms are not available for the general public use and are designated for specific purposes. However, public use of computers and networks may be essential to the operations of the College. Public access may include, but is not limited to, access that is supportive of Admissions, Financial Aid, Career Center Activities, the LSSC library, open computer labs and kiosks.

b. The mission of the LSSC libraries includes providing community user's access to the resource and facilities of the College libraries in support of the College mission to provide cultural, social, and community service activities that enrich the lives of local residents. The Leesburg campus library serves the public as a designated U.S. government document depository library. According to depository law, access to federal government documents must be available to any requestor. LSSC libraries that function as joint-use public library facilities must directly support the general public. The libraries' public access catalog, many government publications and general reference sources are accessible only via the Internet. Therefore, Internet access in college libraries will be available to the general public, at the discretion of the library staff, to provide appropriate information resources to the general public.

c. The open computer labs are designed to serve the computer needs of the students at LSSC. Resources are available for research purposes and for personal use in accordance with the College's policies regarding those resources. LSSC students are LSSC's main priority; however, public access is available on a space-available basis.

VI. SECURITY

a. The LSSC IT department employs various measures to protect the security of its users' accounts and its Information Technology Systems resources. Users are not permitted to share account or password information. Users will be required to change their passwords at intervals determined by the Information Technology Security Committee. As additional technological solutions become available, the LSSC IT department will require additional levels of account security including but not limited to, multi-factor authentication.

b. Users must ensure that they do not violate the conditions of the State and Federal laws dealing with users' right to privacy.

c. Users are prohibited from impersonating any person or entity including accessing others' accounts without authorization, falsely stating or otherwise misrepresenting affiliation with a person or entity, or forging headers or otherwise manipulating identifiers.

d. Users are prohibited from consuming large amounts of bandwidth without authorization so as to interfere with the normal functioning of IT Systems resources, including but not limited to downloading large files or programs, playing online games, accessing streaming audio or video or using the telecommunications system for an unwarranted amount of time, except in designated areas or for legitimate academic purposes.

e. Users are prohibited from engaging in commercial solicitation using IT Systems resources, such as soliciting for advertisers or sponsors or transmitting any unsolicited or unauthorized advertising, phishing emails or emails that are part of any ransomware attacks, bulk mail, spam, chain letters, payment schemes, promotional material or junk mail.

f. Users are not permitted to disrupt classrooms, labs or libraries, for example, by causing computers to display objectionable materials, setting passwords so as to block others from using a computer, or allowing personal electronic devices to sound.

g. Though the LSSC IT department employs various measures to protect the security of its resources, since computers and resources are located in the public areas, the College cannot guarantee privacy or confidentiality. Users should exercise caution when transmitting personal or financial information via IT System's resources. Examples include, but are not limited to:
   1. Identification number, such as Social Security number or LSSC generated ID's;
   2. Credit card or other financial information;
   3. Address or telephone number.

h. As voluntary users, Internet researchers are responsible for defining the constraints of their information searches. The College shall not be held accountable for the accuracy or decency of the data retrieved by public users via the Internet.

VII. TRAINING REQUIREMENTS

a. All awareness training must fulfill the requirements for the Security Awareness Program as listed below:

   The Security Awareness Program should ensure that all staff achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.

   Additional training is appropriate for staff with specific obligations towards information and data security that are not satisfied by basic security awareness, for example Information Risk and Security Management, Security Administration, Site Security and IT/Network Operations personnel.

Security awareness and training activities should commence as soon as practical after a staff or faculty member joins the organization, generally through attending information security induction/orientation as part of the on boarding process. The awareness activities should continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness.

The LSSC IT team can communicate and detail the locations of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters with its employees.

b. LSSC Security Awareness Program

The IT and HR departments will coordinate with and utilize the Lakehawk Leadership Academy to offer Security Awareness Training for each employee upon hire and at least annually thereafter. Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire or as necessary due to IT security violations. Staff will be given a reasonable amount time to complete each course so as to not disrupt business operations.

c. Compliance & Non-Compliance with the Security Awareness Program

Compliance with this program is mandatory for all staff, including contractors and executives. The LSSC IT department will monitor compliance within this program and report to the executive team the results of training and social engineering exercises.

The penalties for non-compliance are described in Section VIII. Violations and Appendix A at the end of this documentation.

d. Non-Compliance Actions

Certain actions or non-actions by LSSC personnel are tracked by our IT department and may result in a non-compliance event (Failure).

A Failure includes but is not limited to:

- Failure to complete required training within the time allotted
- Failure of a social engineering exercise

Failure of a social engineering exercise includes but is not limited to:

- Clicking on a URL within a phishing test;
- Replying with any information to a phishing test;
- Opening an attachment that is part of a phishing test;
- Enabling macros that are within an attachment as part of a phishing test;
- Allowing exploit code to run as part of a phishing test;
- Entering any data within a landing page as part of a phishing test;

- Transmitting any information as part of a vishing test;
- Replying with any information to a smishing test;
- Plugging in a USB stick or removable drive as part of a social engineering exercise;
- Failing to follow LSSC policies in the course of a physical social engineering exercise.

Certain social engineering exercises can result in multiple Failures being counted in a single test. The maximum number of Failure events per social engineering exercise is two.
The LSSC IT department may also determine, on a case by case basis, that specific Failures are a false positive and should be removed from that staff member's total Failure count.

e. Compliance Actions

Certain actions or non-actions by LSSC personnel may result in a compliance event (Pass).
A Pass includes but is not limited to:

- Successfully identifying a simulated social engineering exercises;
- Not having a Failure during a social engineering exercise (Non-action);
- Reporting real social engineering attacks to the IT department via the Phishing Hook or Help Desk tickets.

Each Failure will result in a Remedial action as described in Appendix A of this document. Subsequent Failures will result in escalation of training or coaching.

VII. FEES

Fees or charges billed to LSSC incurred by uses other than official College business may be billed back to the individual responsible. Examples of such fees are personal long distance or cell phone calls, unauthorized use of toll numbers, or other telecommunications charges or costs involved with technology. Users will be financially liable for costs associated with altering, modifying, destroying or taking information resource equipment or supplies without proper authorization.

VIII. VIOLATIONS

The purpose of this procedure is to establish guidelines and ensure that these guidelines are followed by all departments and individuals at LSSC including students, employees, visitors, vendors, or anyone using technology provided by LSSC. This policy applies to all users. If an individual, department, or external entity violates these policies and procedures, whether knowingly, or unknowingly, then the enforcement of such violation may include but not limited to:

1. Disciplinary action, up to and including immediate termination of employment;
2. Disciplinary action including expulsion from the College, if a student;
3. Reimaging of user's computer due to compromise twice within 6 months will result in DeepFreeze locking the workstation down to prevent further infections and/or compromises (minimum of one year of DeepFreeze implementation);
4. Termination of vendor contract or service agreement;
5. Prosecution to violations of the Law.

Appendix A – Schedule of Actions for IT Security Failures

LSSC staff may be required to complete remedial training courses due to test phishing failures or may be required to participate in remedial training exercises with members of the LSSC IT department as part of a risk-based assessment.

The following table outlines the penalty of non-compliance with this program. Steps not listed here may be taken by the LSSC IT team to reduce the risk that an individual may pose to the LSSC. This includes, but is not limited to, locking the employee's active directory account when the employee does not complete the required training within the required time frame.

Failure rates are reset with the annual training period in September.

Failure Count	Resulting Level of Remediation Action
First Failure	Mandatory completion of Remedial Training I and recommended Lake Hawk Academy trainings within 2 weeks of the failure.
Second Failure	Mandatory completion of Remedial Training II and recommended Lake Hawk Academy trainings with 1 week of the failure.
Third Failure	Mandatory completion of Remedial Training III and recommended Lake Hawk Academy trainings within 1 week of the failure. Employee supervisor is notified via email.
Fourth Failure	HR works with supervisor to begin progressive discipline process (Admin Pro 5-25) for a verbal warning with 90-day check in period.
Fifth Failure	HR works with supervisor to provide a written warning to the employee.

Appendix B – Methods for Determining Staff Risk Ratings

The following is a list of situations that may increase a risk rating of a LSSC staff member. Higher risk ratings may result in an increased sophistication of social engineering tests and an increase in frequency and/or type of training and testing.

- Staff member email resides within a recent Email Exposure Check report
- Staff member is an executive or VP (High value target)
- Staff member possesses access to significant LSSC confidential information
- Staff member uses their mobile phone for conducting work-related business
- Staff member possesses access to significant LSSC systems
- Staff member has repeated LSSC Security Awareness Program violations