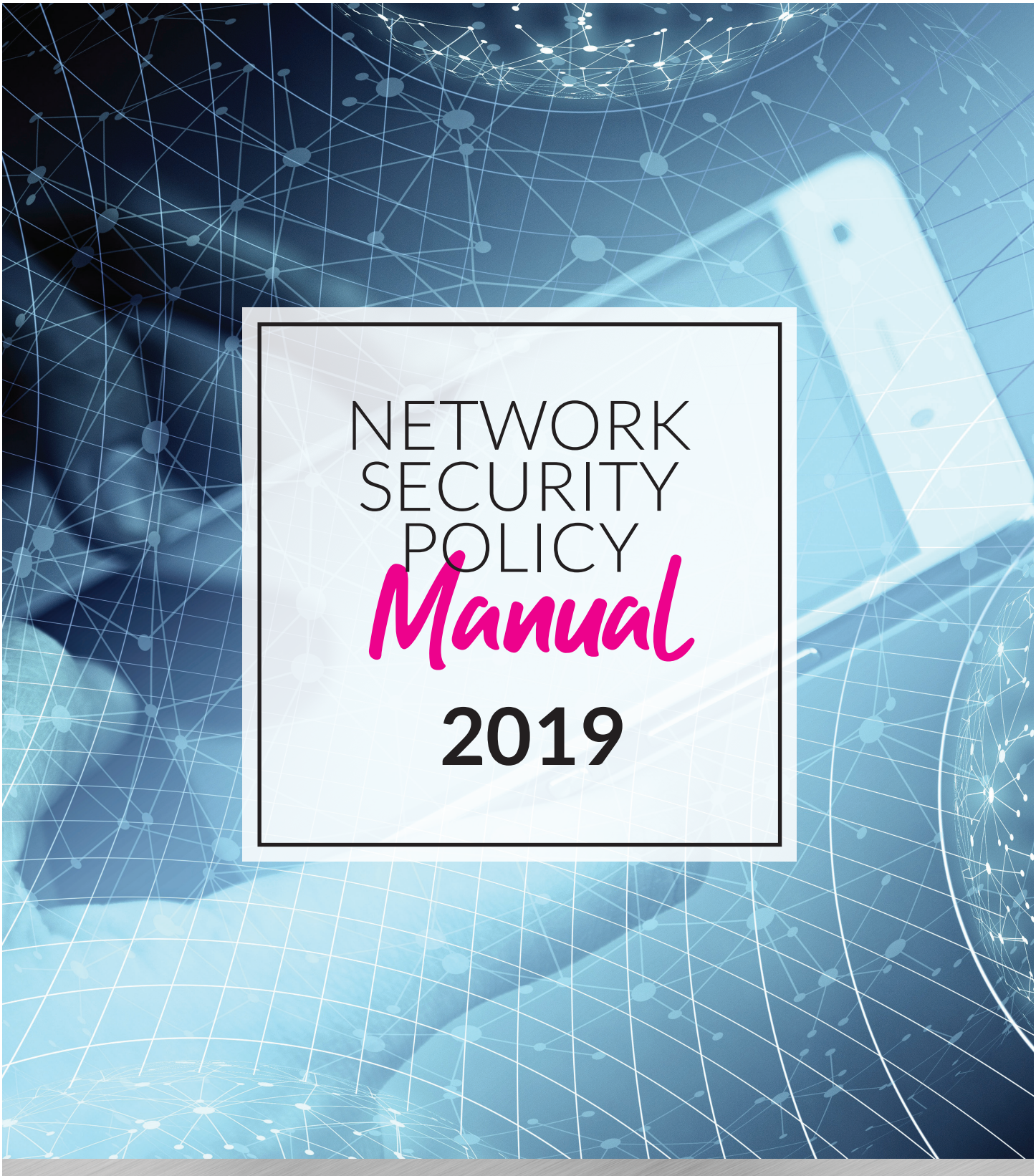

NETWORK SECURITY POLICY Manual 2019

TENAJ
SALON INSTITUTE®

All services performed by supervised students.
Licensed by the Florida Commission for Independent Education. Lic. #3387.

TENAJSALONINSTITUTE.EDU

Follow us: @ tenajsaloninstitute

AACS · nac cas · Federal Student Aid — An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of the AMERICAN MIND®

NETWORK SECURITY POLICY MANUAL

Responsible Division/Office:	Network Security Department
Responsible Officer:	Ruben Zavarce, Chief Information Officer (CIO)
Created:	December 15, 2019
Next Review:	December 2020

Contents

A. POLICY STATEMENT

This Network Security Policy Manual for the Shear Express, Inc. family of business including ZWP, LLC dba Tenaj Salon Institute, Salon Fifth Avenue, LLC dba Salon Jaylee @ Rolling Acres, Dimension Hair Studio, LLC dba Salon Jaylee @ Colony Plaza, Root 466 Salon, LLC dba Salon Jaylee @ Southern Trace and Tenaj Beauty Group, LLC collective referred to herein as the "Company" is intended to be used for the educational and business purposes of the Company in compliance with this policy.

B. SCOPE

This policy applies to all users and uses of Company-owned technology resources as well as to any non-Company and/or remote technology devices while connected to the Company's network.

C. PARAMETERS

1) Technology resources (computing, networking, data and network services) are provided to the Company community in order to fulfill the mission of the Company.
2) While the Company recognizes the importance of academic freedom and freedom of expression, as a Title IV school, the Company also has a responsibility to comply with all federal and state laws and regulations, as well as the obligation to fulfill its mission.
3) Use of Company-owned technology to access resources other than those supporting the administrative, educational, and services missions of the Company or for more than limited, responsible personal use conforming to this policy is prohibited.
4) Technology resources provided by the Company are the property of the Company.

Company-owned technology is not intended to supersede the need for technology purchases for personal purposes.

5) Use of technology is subject to the requirements of legal and ethical behavior and is intended to promote a productive educational and work environment.

D. USER REQUIREMENTS

All users of the Company-owned technology resources (computing, networking and data), regardless of affiliation with the Company, must:

1) Use only those technology resources that they are authorized to use and use them only in the manner and to the extent authorized.
2) Protect the confidentiality, integrity and availability of technology resources.
3) Comply with all federal, Florida, and other applicable law as well as applicable regulations, contracts, and licenses.
4) Comply with all applicable policies of the Company.
5) Respect the right of other technology users to be free from harassment or intimidation.
6) Respect copyrights, intellectual property rights, and ownership of files and passwords.
7) Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.
8) Respect the finite capacity of technology resources and limit use so as not to consume an unreasonable amount of or abuse those resources or to interfere unreasonably with the activity of other users or to disrupt the authorized activities of the Company.
9) Limit personal use of Company technology resources so that such use does not interfere with one's responsibilities to the Company.
10) Not attempt to circumvent information technology security systems or the Company's "Network Security Policy Manual."
11) Not use any radio spectrum space or hotspot on any Company-owned or Company-occupied property, unless it is part of an approved wireless services deployment by the Company.
12) Not use technology resources for personal commercial purposes or for personal financial or other gain unless specifically approved by the Company.
13) Not state or imply that they speak on behalf of the Company without authorization to do so and not use Company trademarks and logos without authorization to do so.

E. USER RESPONSIBILITIES

1) By accepting employment, being admitted as a student, or asking for any guest technology resource privileges, users implicitly agree to adhere to this policy and agree to adhere to the Company's "Network Security Policy Manual."
2) Users are responsible for any activity performed using their usernames and passwords except when account security is compromised by actions beyond the user's control.
3) Users are responsible for any activity performed on Company-owned technology devices assigned to them except when the device is compromised by actions beyond the user's control.
4) There is no expectation of personal privacy when using Company resources. (See paragraph F of this rule.)
5) Potential violations regarding use of technology resources should be reported to the appropriate information technology services manager(s) or information security officer.

6) Users are responsible for ensuring that critical data are backed up and available to be restored for systems not administered by information systems technology. This includes critical information contained on technology devices oriented to individual use (e.g., desktops, laptops, smart phones, and similar such devices).

7) Users are responsible for maintaining data in compliance with the Company records retention plan.

8) Users are responsible for ensuring that sensitive information to which they have access is guarded against theft.

9) Personal use of computing resources not otherwise addressed in this policy or these procedures will generally be permitted if such use does not consume a significant amount of resources, does not interfere with the performance of an individual's job or other Company responsibilities, and is otherwise in compliance with Company policies.

F. NO EXPECTATION OF PRIVACY

1) The Company does not routinely monitor specific individual end-user usage of its technology resources. However, the Company does routinely monitor technology resource usage in the normal operation and maintenance of the Company's computing, network and data resources. This monitoring includes the caching and backing up of data and communications, the logging of activity, the monitoring of general usage patterns, the scanning of systems and networks for anomalies and vulnerabilities, the filtering of malicious traffic, and other activities that are necessary for the rapid and efficient delivery of services. Technology users should be aware that there is no expectation of privacy associated with the use of Company technology resources.

2) The Company may also specifically monitor the activity and accounts of individual end-users of Company technology resources, including login sessions, file systems, and communications.

3) When authorized by the appropriate Company administrator (Chief Executive Officer or Chief Operating Officer), the Company may access active end-user accounts, files, or communications used for Company business when needed by a supervisor or assigned personnel for Company business and the end-user is unavailable. For inactive end-users, such as retirees or terminated employees, the end-user's former supervisor or the individual currently holding the supervisor position may request access. For inactive end-users the provost may authorize access. For all other inactive end-users, the general counsel may authorize access.

4) The Company, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate Company personnel or law enforcement agencies and may use those results in appropriate Company disciplinary proceedings.

5) Personal computing devices:

   a) Personal computing devices (laptops, desktops, tablets) are restricted to the Company wireless network)

   b) No personal computing devices will be allowed to connect to the wired Company network.

   c) Personal computing devices must comply with the Company's Network Security Policy Manual when using the campus wireless network or other provided Company technology resource.

   d) Personal computing devices used to conduct Company business are subject to these policies.

e) Personal hubs, routers, switches, or wireless access points are prohibited from being connected to either the Company's wired or wireless network.

G. EMAIL

Email is an official means for communication at the Company. faculty, and staff are expected to check their official email address on a frequent and consistent basis in order to stay current with Company communications.

H. SECURITY

The Company employs various measures (i.e., the Company's "Network Security Policy Manual") to protect the security of information technology resources and user accounts; however, users should be aware that the Company cannot provide good security without user participation. Users should increase their technology security awareness and fully employ access restrictions for their accounts, including using strong passwords, guarding passwords diligently and changing passwords regularly to help safeguard their use of technology.

I. ADDITIONAL POLICY RAMIFICATIONS

Users must abide by all applicable restrictions, whether or not they are built into the computing system, network or information resources and whether or not they can be circumvented by technical or other means. Individuals who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those states and countries and the rules and policies of those technology systems and information resources.

J. EXAMPLES OF UNACCEPTABLE USE

1) As a further aid to policy compliance, the following non-exhaustive list is provided of activities that are prohibited.
   a) Using technology resources to engage in fraud, defamatory, abusive, unethical, indecent, obscene, pornographic and/or unlawful activities is prohibited.
   b) Using technology resources to procure, solicit, or transmit material that is in violation of sexual, racial or other harassment or hostile workplace laws is prohibited.
   c) Any form of harassment by electronic means (e.g., email, web access, phone, paging), whether through language, content, frequency or size of messages is prohibited.
   d) Making fraudulent offers of products, items or services using any Company technology resource is prohibited.
   e) Using technology resources for unauthorized or inappropriate financial gain, unauthorized solicitation, or activities associated with a for-profit business, or engaging in an activity that involves a conflict of interest.
   f) Creating or forwarding chain letters, Ponzi, or other pyramid schemes is prohibited.
   g) Broadcasting of unsolicited mail or messages is prohibited. Examples include chain letters, virus hoaxes, spam mail, and other email schemes that may cause excessive network traffic. Sending large numbers of electronic mail messages for official Company purposes necessitates following the Company's procedures for the electronic distribution of information.
   h) Sending junk mail or advertising material to individuals who did not specifically request such material (email spam) is prohibited.

i) Violations of the rights of any person or Company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed is prohibited.

j) Unauthorized copying and downloading of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and films and the installation of any copyrighted software for which an active license has not been procured is prohibited.

k) Circumventing user authentication or security of any host, network or account is prohibited. This includes, but is not limited to, monitoring by use of keylogging or session logging.

l) Revealing your account password to others or allowing use of your account by others is prohibited. This prohibition extends to family, other household members, friends and/or co-workers.

m) Attempting to log onto another user's account (secured or otherwise) is prohibited.

n) Sending electronic communications in such a way that masks the source or makes it appear to come from another source is prohibited.

o) Personal use beyond limited responsible use is prohibited.

2) Exemptions. Individual Company staff may be exempted from these restrictions on a case-by-case basis (with written authorization according to the Company's "Network Security Policy Manual") in the course of performing legitimate job responsibilities.

3) Passwords. Special procedures exist and must be followed to ensure that accounts for employees are secured with passwords known to only the account holder. Passwords may be changed at the request of the area supervisor and approved by the supervisor's vice president or the president.

4) Under no circumstances is an employee of the Company authorized to engage in any activity that is unethical or illegal under local, state or federal law while utilizing Company-owned resources.

K. ENFORCEMENT

1) The office of the Chief Technology Officer may suspend and/or restrict either an individual's or a device's access to the Company network resource if:

a) It is deemed necessary to maintain the security or functionality of the network resource.

b) It is deemed necessary to protect the Company from potential liability.

c) The account, system, or device is believed to have been either compromised or is in violation of this policy.

2) The office of the chief technology officer must immediately report the enforcement action and the justification for the action to the Chief Excitative Officer or Chief Operating Officer of student (or their designee), as applicable. The Company may permanently suspend all technology access of anyone using the Company network resource until due process has been completed the employees' administrative discipline and/or law enforcement agencies.

L. PASSWORDS

The Company Password Policy establishes the position that poor password management or construction imposes risks to the security of Company information systems and resources. Standards for construction and management of passwords greatly reduce these risks.

1) Objective / Purpose

This document describes the acceptable standards for password construction and management.

2) Scope

The requirements in this standard apply to passwords for any computing account on any Company computer resource, to the users of any such accounts, and to system administrators and developers who manage or design systems that require passwords for authentication.

3) Standard

a) Minimum Password Length

Passwords shall have a minimum of 10 characters with a mix of alphanumeric and special characters; if a particular system will not support 10-character passwords, then the maximum number of characters allowed by that system shall be used.

b) Password Composition

Passwords shall not consist of well-known or publicly posted identification information. Names, usernames such as the MyID, and ID numbers such as the 81x or COMPANYID number are all examples of well know identification information that should not be used as a password.

c) Password Storage

Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames.
Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to said application.

d) Password History

Users will be prohibited from re-using the last 5 previously used passwords.

e) Password Reuse

Care shall be taken to prevent the compromise of one username/password from compromising the security of multiple systems or resources. The username and password(s) used for your COMPANY accounts should never be used for any other non-COMPANY accounts and services.

f) Password Sharing and Transfer

Passwords shall not be transferred or shared with others unless the user obtains appropriate authorization to do so.
When it is necessary to disseminate passwords in writing, reasonable measures shall be taken to protect the password from unauthorized access. For example, after memorizing the password, one must destroy the written record.
When communicating a password to an authorized individual orally, take measures to ensure that the password is not overheard by unauthorized individuals.

g) Electronic Transmission

Passwords shall not be transferred electronically over the Internet using insecure methods. Wherever possible, security protocols including IMAPS, FTPS, HTTPS, etc. shall be used.

h) Exceptions

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. To request a security exception, contact the Chief Technology Officer.

4) Acceptable Methods to Create a Strong Password

a) Use a minimum of 10 characters. Generally, the more characters you can use, the harder a password is to be cracked or guessed.

b) Choose a password that is easy for you to remember but would be hard for another to guess. One useful approach is to use a sentence or saying to create a "passphrase" by using the first letters, capitalization, and special characters as substitutes. For example, "One ring to rule them all, one ring to bind them" may be used to create a passphrase like "1R2rtAor2Bt" that can be used as a very strong password.

c) Passwords must include at least three of the four following types of characters

d) English uppercase letters (A through Z).

e) English lower-case letters (a through z).

f) Numbers (0 through 9).

g) Special characters and punctuation symbols (Example: _, -. +, =,!, @, %, *, &, ", :, ., or /).

h) Do not use the following characters \ , ~ or < .

i) Do not use a space or tab.

j) Reuse of any of your last 5 passwords is prohibited.

5) Tips for Creating a Strong Password

a) Avoid words, numbers, or known or public information associated with you. (e.g. Social security numbers; Names, family names, pet names; birthdays, phone numbers, addresses; etc.)

b) Avoid using your login name or any variation of your login name as your password. If your login is 'fredrick', do not use substitution or letter reordering. Examples would be 'fr3dr1ck', where the 3=e and the 1 (one)= i. Alternatively, do not use kcirderf (backwards) or add a digit to the beginning or end of the word (1fredrick or fredrick1).

c) Avoid using the same character for the entire password (e.g., '11111111') or using fewer than five unique characters.

d) Avoid common letter or number patterns in your password (e.g., '12345678' or 'abcdefgh'). They are the first things hackers will test.

e) Substitution should not be used on common words or with common substitutions (e.g., 3=E, 4=A, 1=I, 0=O, etc).

f) When changing a password, change to an entirely new password. Do not just rotate through a list of favorite passwords.

NOTES

NOTES

THE BIGGEST ADVENTURE YOU CAN TAKE IS TO LIVE THE LIFE OF YOUR... *Dreams!*

- Oprah

NSPM, EFFECTIVE DECEMBER 04TH, 2019

TENAJ
SALON INSTITUTE®

11915 CR 103
THE VILLAGES, FL 32162
352.753.5511
352.259.6712
TENAJSALONINSTITUTE.EDU