1. POLICY STATEMENT

Technical security controls are a vital part of our information security framework; however, they are not sufficient to secure all of The Community Solution Education System's ("The System" or "System") information and data without employees being thoughtful in the way they handle and protect information. Effective information security requires the awareness and support of all staff to identify threats that are not detected by available technology controls. Risks frequently occur in the form of Social Engineering attacks, Spam, and other Malware attacks which specifically target humans rather than technology.

Compliance with this Privacy and User Awareness and Training Policy ("Policy") is **mandatory** for all Users, as defined in the Definitions section. The System will monitor compliance and non-compliance with this policy and may report the results of training and Social Engineering exercises to managers, department heads, the President of the System, or the President's Direct Reports.

2. PURPOSE

This Policy is a component of the System's security program. It sets forth the internal information security awareness and training that is designed to inform all Users about their obligation to keep System information secure. By completing ongoing training, Users will become increasingly more knowledgeable about potential cyber threats and will learn about the training tools designed to defend against these threats.

3. APPLICABILITY

This policy applies to all Users, as defined in the Definitions section.

4. DEFINITIONS

4.1 Social Engineering

A term used for maliciously using human interaction to trick Users into making security mistakes or giving away data to any individual(s) not authorized to possess such data.

4.2 User(s)

Any person who possesses an active email account that is managed by the System's Information Technology department. This includes full-time, part-time, and temporary employees. It excludes Students.

4.3 Phishing

An attempt by a malicious actor to harm a company or individual by obtaining sensitive information through email.

4.4 Spam

Unsolicited email used as a means of selling products or services to a large market of buyers. This is also referred to as "junk mail."

4.5 Highly Sensitive Data

Highly Sensitive Data means Personal Information that may cause serious and potentially irreparable harm to a User if disclosed or used in an unauthorized manner.

4.6 Personal Information

A User's name, or any other direct or indirect identifier of an individual, in combination with any one or more of the following data elements about the individual:

- Social security number
- Driver's license number or state identification card number
- Passport or Foreign Visa number
- Financial account number, or credit card or debit card number
- FERPA education record information
- Protected health information

4.7 Malware

This term is short for malicious software and refers to computer programs designed to alter computers in a damaging way without users' consent. Malware is a broad term that covers different types of threats, such as viruses, spyware, worms, trojans, rootkits, and others.

4.8 Information Asset

Information Asset as it pertains to organizational risk, is information or data that is of value to the System, including but not limited to personal health information, intellectual property, personally identifiable information, student financial information, credit card information or customer information that requires protection. Information Assets can be in the form of paper, CD's, or other media stored electronically on databases, files, or personal workstations and System workstations.

5. PROCEDURES

The first line of defense for Phishing and Social Engineering attacks is the User. The goal of User awareness and training is to educate Users on the various tools, tactics, and procedures that attackers use to engage and trick Users into performing an action that is damaging to themselves or to the System. The System will provide Users with training that will focus on Social Engineering and Phishing campaigns and may address other topics as new threats emerge. It is mandatory for Users to complete such training and any necessary retraining within the timeframe announced.

5.1. Training Exercises

The System will periodically send Users training in the form of a link in an email. Training frequencies are based on current and trending threats as it relates to Phishing and Social Engineering attacks. Training links will be sent to the User's inbox in an email and will direct the User to their personal training web portal, which will outline:

- Current training videos and/or documents and deadlines to complete the required training.
- Any policies that are required to be formally acknowledged.

5.2. Testing

Users will be tested on their understanding of training exercises. During and/or after training exercises, Users may be asked questions that require an answer before moving on. The results of whether the test taker passed the test or failed will be logged for review. Those who can review test results include the User who took the test, managers, department heads, President's Direct Reports and the President of the System.

5.3. Simulated Phishing Campaigns

Simulated Phishing campaigns are safe phishing attacks that are sent by information technology staff to gauge a User's effectiveness at spotting a phishing email. TCS will engage in simulated Phishing campaigns designed to give information technology staff results based on the User's response, to be used to tailor future training exercises.

5.4. Supplemental Training

Supplemental training may be provided to develop additional User awareness materials regarding Social Engineering and Phishing techniques beyond training exercises. Supplemental training does not test the User. Its purpose is to provide materials for additional learning on current and trending scams and are not part of mandatory training.

5.5. Disciplinary Action

All Users who are employees of the System are required to adhere to this Policy as a condition of their continued employment. Any User that does not comply with this Policy will be referred to their supervisor for disciplinary action. Third party Users that do not comply with this Policy may be subject to having their System email accounts disabled.

5.6. Compliance with Policies

Users agree that their use of the System's IT resources is subject to this Policy and any

additional policies, procedures, standards, and processes the System implements, including but not limited to, the Highly Sensitive Data Policy, Privacy and User Awareness and Training Policy, Data Incident Notification Policy, Mobile End-User Device Policy, and Social Media Policy

6. RELATED DOCUMENTS

- Highly Sensitive Data Policy
- Computer & Email Usage Policy
- Mobile End-User Device Policy
- Password Management Policy

7.CONTACTS

- Manager, Information Security