Online Auction

Updated Security Manual



**Slippery Rock University of Pennsylvania**

Contributions by:

**Fall 2023**

Timothy Holtz – tth1003@sru.edu

Douglas Maxwell – dsm1015@sru.edu

Luke McElligott – lpm1006@sru.edu

Table of Contents

[Scope 3](#_Toc152009875)

[Confidential Data 3](#_Toc152009876)

[Protect personal and company devices: 3](#_Toc152009877)

[Logging: 4](#_Toc152009878)

[Keep Emails Safe 4](#_Toc152009879)

[Managing Passwords Properly 4](#_Toc152009880)

[Two-Factor Authentication 5](#_Toc152009881)

[Transfer Data Securely 5](#_Toc152009882)

[Additional Measures 5](#_Toc152009883)

[Take Security Seriously 6](#_Toc152009884)

Policy Brief & Purpose

The purpose of this manual is to ensure that cybersecurity threats are minimized. Offerly uses technology to collect, store, and manage information which can increase the chance of a severe security breach. For this reason, many security measures have been implemented.

## Scope

These policies applies to all employees, contractors, volunteers, and anyone who has permanent or temporary access to our systems and hardware.

### Confidential Data

Confidential Data is secret and valuable. All employees are obliged to protect this data.

To protect and uphold the integrity of information of the user, a newer system with updated security features had been implemented. A user seeking to add or edit personal information will be prompted to submit their relevant credentials to prevent change of information by an outside entity.

### Protect personal and company devices:

When employees use their devices to access company emails or accounts, they introduce security risks. The company advises our employees to keep both their personal and company-issued computer, tablet, and cell phone secure. Offerly employees should avoid logging on to their accounts from other people’s devices or lending their own to others. Below are ways that employees can keep their devices secure:

* Keep all devices password protected.
* Choose a reputable antivirus software.
* Ensure they do not leave their devices exposed or unattended.
* Install security updates of browsers and systems monthly or as soon as updates are available.
* Log into company accounts and systems through secure and private networks only

### Logging:

Another security method that has been implemented into the project is event logging and monitoring. Activity logging greatly increases the security of the application as user activity is recorded and stored so in the event that there is a security incident, the logs can be reviewed to show how the system was exploited.

Logs are recorded during most user actions (such as buying, bidding, messaging, etc.) and can be viewed by administrative accounts. Admin accounts can find a “Logs” tab in the web interface which brings them to a page where logs can be monitored. From here, logs can be filtered and sorted to the administrator’s needs.

### Keep Emails Safe

Emails are often social engineering scams or are inflicted by malicious software (e.g., worms.) To avoid virus infection or data theft, we implore employees to:

* Avoid opening attachments and clicking on links when the content looks too good to be true or far-fetched (e.g., “Congratulations, you won our giveaway!”).
* Be suspicious of clickbait titles (e.g., offering prizes, advice).
* Check the names and email addresses of people that sent the message to ensure they are legitimate.
* Look for inconsistencies (e.g., grammar mistakes, capital letters, excessive number of exclamation marks).

Phishing threats greatly threaten a company’s data and therefore phishing policies are essential.

### Managing Passwords Properly

Password leaks are dangerous since they can compromise the entire business. Leaked passwords can lead to ransomware attacks and compromised data. Not only should passwords be secure, but they should also remain secret. For this reason, we advise our employees to:

* Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g., birthdays, relative’s names, etc.).
* Remember passwords instead of writing them down.
  + A reputable and secure password manager may also suffice.
* Exchange credentials only when necessary.
* Change their passwords every two months.

### Two-Factor Authentication

In order to enhance the security of the online auction platform, two-factor authentication has been implemented into Offerly. This decision was made to increase security of the platform as:

* User accounts will now need to provide two means of authentication before being able to login.
* Consumer trust will be increased.
* In the future, it may provide compliance or single sign-on (SSO) capabilities.

Implementing two-factor authentication greatly reduces Offerly’s attack vector from login-related threats.

### Transfer Data Securely

Transferring data introduces security risk. Employees must:

* Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless necessary.
* Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
* Report scams, privacy breaches and hacking attempts.

Offerly needs to know about scams, breaches, and malware so that the company can better protect the infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails, or phishing attempts as soon as possible.

### Additional Measures

To reduce the likelihood of security breaches, we also instruct our employees to:

* After 5 minutes without activity on the webpage, administrators will be unable to make changes until they successfully re-validate credentials.
* Report stolen or damaged equipment.
* Change all account passwords when a device is stolen.
* Report a perceived threat or possible security weakness!
* Refrain from downloading suspicious, unauthorized, or illegal software.
* Avoid accessing suspicious websites.

### Take Security Seriously

Our customers should feel that their data is safe. Employees should be vigilant by proactively protecting Offerly’s systems and databases. To ensure trust, employees should keep cybersecurity a priority.