Online Auctioning

Security Manual

**Slippery Rock University**

Spring 2024

Jacob Johnston – jrj1014@sru.edu

Tiffany Morrow – tbm1005@sru.edu

Nicholas Vioral – ncv1005@sru.edu

Wolfgang Zoppelt – wsz1001@sru.edu

Policy Brief

This manual aims to reduce cybersecurity risks by implementing various security measures due to Offerly's utilization of technology for gathering, storing, and handling information, which heightens the risk for potential security breaches.

Scope

These policies are applicable to every employee, contractor, volunteer, and individual with either permanent or temporary access to our systems and hardware.

Confidential Data

Confidential data is both secret and valuable, and it is the responsibility of all employees to safeguard it.

To maintain the integrity of user information, a new system with updated security features has been implemented. Users who wish to add or modify personal information will be required to provide their relevant credentials to prevent unauthorized changes by external entities. Ensuring the security of personal and company devices is crucial.

When employees use their devices to access company emails or accounts, they introduce potential security vulnerabilities. Therefore, the company advises all employees to maintain the security of both their personal and company-issued computers, tablets, and cell phones. Offerly employees should refrain from logging into their accounts using others' devices or lending their devices to others. Below are some methods employees can employ to secure their devices:

⦁ Ensure all devices are password protected.

⦁ Select reliable antivirus software.

⦁ Avoid leaving devices exposed or unattended.

⦁ Regularly install security updates for browsers and systems, either monthly or immediately upon availability.

⦁ Access company accounts and systems only through secure and private networks.

Implementing activity logging significantly enhances the application's security by documenting and storing user actions. In case of a security breach, these logs can be reviewed to identify how the system was compromised.

Logs are generated for various user interactions, including purchases, bids, messaging, and more. Administrative accounts have access to view these logs through a designated "Logs" tab in the web interface. This feature allows administrators to monitor logs, filter, and sort them according to their requirements.

Credential Safety

Emails often serve as conduits for social engineering scams or malicious software. To prevent virus infections or data breaches, we strongly advise employees to:

⦁ Exercise caution when encountering attachments or links in emails that seem too good to be true or overly sensational (e.g., "Congratulations, you've won our giveaway!").

⦁ Remain wary of clickbait subject lines (e.g., promises of prizes or advice).

⦁ Verify the legitimacy of senders by scrutinizing their names and email addresses.

⦁ Watch out for inconsistencies in the email content, such as grammar errors, unusual capitalization, or excessive use of exclamation marks.

Phishing threats pose significant risks to a company's data, underscoring the importance of implementing robust phishing policies.

The exposure of passwords poses significant risks as it can jeopardize the entire business. Such breaches may result in ransomware attacks and compromised data. It's crucial not only to create secure passwords but also to keep them confidential. Therefore, we recommend the following practices to our employees:

⦁ Opt for passwords comprising a minimum of eight characters, incorporating a mix of uppercase and lowercase letters, numbers, and symbols, while avoiding easily guessable information like birthdays or relatives' names.

⦁ Commit passwords to memory rather than writing them down.

⦁ Consider utilizing a reputable and secure password manager.

⦁ Share credentials only when necessary.

⦁ Regularly update passwords every two months.

Data Transfer Policy

The process of data transfer poses inherent security risks. Therefore, employees should:

⦁ Refrain from transferring sensitive data, such as customer information or employee records, to other devices or accounts unless it is absolutely necessary.

⦁ Verify that recipients of the data are duly authorized individuals or organizations with sufficient security protocols in place.

⦁ Promptly report any instances of scams, privacy breaches, or hacking attempts.

Offerly relies on awareness of scams, breaches, and malware to enhance its infrastructure's protection. Consequently, we encourage employees to promptly report any perceived attacks, suspicious emails, or phishing attempts to ensure swift action can be taken.

Additional Proceedures

To minimize the risk of security breaches, we provide the following guidelines to our employees:

⦁ Administrators will be required to re-validate credentials after 5 minutes of webpage inactivity before making any changes.

⦁ Promptly report any instances of stolen or damaged equipment.

⦁ Change all account passwords if a device is stolen.

⦁ Report any perceived threats or potential security vulnerabilities.

⦁ Refrain from downloading suspicious, unauthorized, or illegal software.

⦁ Avoid accessing websites that appear suspicious.

It's crucial for our customers to have confidence in the security of their data. Therefore, employees must remain vigilant by actively safeguarding Offerly's systems and databases. Upholding cybersecurity as a top priority is essential to maintaining trust.