# UNIVERSITY DEPOT

Logo, company name

Description automatically generated

**Cybersecurity Manual**

**Slippery Rock University**

Stephen Simpson - sjs1035@sru.edu

Cody Kuntz - cak1033@sru.edu

Heidi Bednarz - heb1010@sru.edu

Dustin Annarumo-dja1011@sru.edu

Zack Colich - zjc1006@sru.edu

Jenna Josselyn jmj1022@sru.edu

Table of Contents

# Policy Brief & Purpose ............................... 3

# Scope .............................................. 3

# Policy Elements .................... 3

# Confidential Data ............................... 3

# Keep Emails Safe .............................................. 4

# Managing Passwords Properly .................... 4

# Transfer Data Securely ............................... 4

# Additional Measures .............................................. 5

# Take Security Seriously .................... 5

Policy Brief & Purpose

University Depot cyber security policy outlines the guidelines for preserving the security of the data and technology infrastructure. The company have also prepared instructions that may help mitigate security risks.

The purpose of this manual is to ensure that cybersecurity threats are minimized. University Depot uses technology to collect, store, and manage information which can increase the chance of a severe security breach. Other factors that could increase the risk are human errors, hacker attacks and system malfunctions which could lead to great financial damage and may jeopardize University Depot’s reputation. For this reason, many security measures have been implemented.

## Scope

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

## Policy Elements

### Confidential Data

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

* Customer’s banking information
* Customer’s username/password
* Customer’s friends
* Selling list

### 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. University Depot 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 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

### 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 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.)

### 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.)
* Remember passwords instead of writing them down
* Exchange credentials only when absolutely necessary
* Change their passwords every two months.

### 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 absolutely 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

University Depot 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:

* Turn off screens and lock devices when leaving desks
* 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 University Depot’s systems and databases. To ensure trust employees should keep cyber security top of mind.