Selflessly - Acceptable Use

Version #0.0.0

- Created: Mon, 02 May 2022 14:51:37 -0400
- Last Modified: Thu, 12 May 2022 15:51:42 -0400

Introduction and Scope

This policy outlines the acceptable use of Selflessly information, electronic and computing devices, and network resources. The policy applies to resources owned or leased or otherwise under contract by Selflessly. Information governed within the scope of this policy includes all company-owned and controlled information as well as all information shared with Selflessly by customers and other stakeholders. Personally owned devices or assets used for work purposes are governed by the Bring Your Own Device (BYOD) Policy.

All employees must follow this policy when they use electronics or networks for Selflessly-related business.

Personal Use of Selflessly Resources

- Good judgment must be used when using company resources for personal use.
- Compliance with company policies and procedures must be practiced at all times.
- Use of company resources may be monitored for security, privacy, and maintenance purposes. Personal use is therefore at the user's own risk.
- Selflessly may audit networks, systems, and hardware at any time to ensure that all devices and systems are in compliance with all Selflessly policies, leveraged standards, and applicable regulations.

Legal Obligations

All employees and contractors must follow copyright, trade secret, patent, privacy, and all other laws or regulations at all times when using Selflessly resources.

In the case that any employees or contractors are unsure whether a resource they are using has a legal obligation such as copyright tied to its use, they have a responsibility to ask their manager for further guidance and direction. If the manager is unsure, the manager shall ask the Security Team for further guidance and direction.

Network, Cloud, and Endpoint Security

These rules about acceptable and unacceptable use will help keep the network, cloud resources, and endpoints secure.

Employees must:

- Only download software that the Security Team has approved.
- Keep their passwords secret, even from coworkers.
- Learn how to identify suspicious email so that they can avoid opening, sending, or forwarding email that contains viruses or malware.

Employees must never:

- Introduce malicious software into any Selflessly devices or systems.
- Let others use their accounts.
- Interfere with or breach the security of network communication, computers, or user sessions.
- Access data meant for others.
- Log in to a server or account without authorization.
- Disrupt Selflessly networks or cloud environments in any unauthorized manner
- Bypass user authentication or security of any computer, network, or account.
- Spoof email addresses.
- Connect network devices to the Selflessly network environment or cloud computing environments without getting proper permission from the Security Team. Devices could include wireless access points, personal laptops, cell phones, or printers.
- Monitor the network unless they need to as part of their normal job requirements.
- Create or forward spam, including chain letters, Ponzi schemes, or other pyramid schemes.
- Market or sell fraudulent products, items, or services.

Exceptions

In the case that an employee requires software by exception or prefers to use software not specifically approved by the Security Team, the employee will, in writing, contact the Security Team to request an exception be made for the software.

The Security Team will perform all necessary due diligence in determining if the software meets Selflessly standards and policies for security, privacy, and third-party risk.

The exception will be recorded for auditing purposes.

General Use of Social Media and Other Personal Use

General use of social media, and company issued hardware, and Wi-Fi access points is permitted providing it follows this policy and does not interfere with one's responsibility and work. Company cloud environments are not to be used for personal matters or any other use case outside of the scope of an individual's roles and responsibilities at Selflessly.

Official Selflessly Social Media Content

Posting of content to corporate sponsored social media (e.g. the corporate Facebook page) is permitted only for the authorized employees.

Email Usage

When sending external email employees must be sure to never include material that would reflect poorly on the reputation of Selflessly, its clients, business partners, and the general public. Selflessly email is not to be used for personal matters and must be exclusively utilized for job-related purposes for which the employee is trained and has the permission to conduct.

The following rules must be followed when using email:

- Selflessly permits sending its highest classification of data internally or to the individual that is the owner, controller, or processor of the data or is otherwise explicitly permitted to receive or access the information.
- Employees must comply with all relevant laws and proper business practices.
- Employees may only use company email accounts for business-related purposes.
- Employees must never set up automatic forwarding from their company email to a personal third-party email system such as Gmail or Outlook.

Use of Email Clients

The use of email clients for sending and receiving correspondence on behalf of Selflessly is limited to fully supported, up-to-date email clients.

Virus and Malware Protection

All employees must keep their assigned email account secure by doing the following:

- Identifying the email's sender before opening it or any attachments
- Double-checking that the email address is accurate to ensure the email is not from a malicious actor who is pretending to be a known trusted person
- Ensuring that email settings are configured so that file types and extensions can be viewed before opening an attachment
- Only opening attachments from trusted individuals
- Never opening suspicious email attachments (e.g., from emails with misspelled subject lines or from institutions that shouldn't have their work email address)
- Reporting any suspicious emails to the Security Team

Definitions

Definitions for terms can be found in the Intercom knowledge base glossary of terms. To access the Glossary, interact with the Intercom speech bubble from any page on the Carbide platform and search for `Glossary.'