Acceptable Use Policy for AppJoy Platform

Joseph Patrick

Liberty University

Studies in Information Security, CSIS 340

February 4, 2023

Acceptable Use Policy for the AppJoy Platform.

**Overview**

This acceptable use policy is in place for the purpose of providing protection and safety to the users of AppJoy, the software distribution app. This policy is meant to embrace the open-source and strong security that we provide at Joseph Corporation. We are dedicated to providing a secure and substantial experience for every user or organization.

Intranets, Computers, Mobile devices, operating systems, network accounts and storage media are the property of AppJoy and are used to best serve the customer with the AppJoy experience. These components are required to provide security and to maintain company policy. Please review Human Resources to find further details relating to devices and device constituents.

Security is the number one priority of AppJoy’s development team and to provide an effective and clear customer experience, every member of AppJoy has completed cybersecurity compliance training. This will not prevent but will reduce the large number of cyber-attacks regarding our applications. We are aware of the threats that are present with downloading software, therefore. These guidelines are required to be read to use the AppJoy on any computer system.

**Purpose**

The purpose of this policy is to outline the acceptable use of the AppJoy platform by The Joseph Corporation. These rules are in place to protect individuals and organizations that have chosen to use AppJoy as their application installation software. AppJoy is dedicated to providing a secure application delivery experience and this includes preventing inappropriate use to defend from viruses and other malware.

**General Objective**

AppJoy’s objective is to provide safe and secure software applications to a broad range of computer systems while retaining proper security and updates to said software applications.

**Intended Use**

AppJoy is intended to be used as either community or enterprise. Community editions of AppJoy provide the same applications and the same security, however, it does not allow for remote management. The enterprise edition of AppJoy comes with the application management suite, and administrator credentials. The application management software allows for an organization to monitor the software installed on every computer.

There will be limitations to AppJoy’s administration tools due to the high likelihood of attackers attempting to hijack these tools. According to Huang, K., Siegel, M., & Madnick, S. , “Hackers can package exploits in an exploit kit to simplify and increase the success rate of attacks.” The packaged exploits mean that if there was unlimited security controls for the organization, they would be more likely to experience a massive attack.

**Scope**

This policy applies to the use of software and information pertaining to the applications that are installed by either the AppJoy Command Line Interface, the AppJoy web interface, or the AppJoy API. Network resources that are needed to provide secure service are also maintained by the AppJoy platform. All employees, contractors, consultants, temporary, and other workers that interact with the AppJoy platform and its subsidiaries are responsible for exercising good judgement and accurate knowledge of all AppJoy policies.

This policy applies to any individual or organization who has impacted the development of the AppJoy platform.

**Policy**

AppJoy CLI downloads will be hosted on our webpage “AppJoy.com”. This is implemented as a security measure to prevent users from accidentally installing counterfeit software. As a user of the AppJoy platform, once an AppJoy subscription has been purchased, or a installment of AppJoy’s community edition, management of software is administered by the organization or individual respectively.

AppJoy is responsible for the security and validity of the software that is hosted on the platform, however there will be periods of time where a software may be unusable due to security constraints. This will only happen in regards to and administrator reporting an incident or concern regarding an application in the AppJoy platform. The programs will be unavailable to use, however they will immediately be saved in a sandboxed environment where testing can occur. After the appropriate checks and procedures are performed on the software, it will then be released back to the client and more heavily monitored should something seem to be potentially harmful.

The unlawful use of AppJoy will be processed as due according to the law at the time of the incident.

**Policy Compliance**

The AppJoy platform policy will be enforced by our monitoring software which is monitored and used to determine whether or not there has been a breach of acceptable use during a user’s AppJoy experience.

**Related Standards**

**Data Classification Policy**

All data that is found within the AppJoy platform are managed by AppJoy and all software that is available for download on the AppJoy platform has been tested and verified by AppJoy. Though the software installers are verified and secure, the information that is present form the applications is not the responsibility of AppJoy to maintain, i.e. If you lose data, or are not able to access data, it is the responsibility of the corresponding application to manage.

AppJoy requires the operating system of the host machine to provide correct installers. Though these installers may be shown as an executable file, they will be downloaded according to the proper operating systems specification.

**Password Policy**

The AppJoy platform requires that all users are authenticated before use. This can either be from the CLI or a web browser. To maintain security, passwords must contain a capital and lowercase letter, a number or special character, and it cannot contain the username in the password body. AppJoy’s cybersecurity team will maintain and monitor the password process. Passwords are required to be reset at a minimum of 1 year from previous set date.

Any compromised passwords are able to be reported to administrators who have the ability to limit the account’s access. If the account is deemed unknown, it can be marked for destruction and AppJoy’s security programs will scan and delete data that the account has created through the AppJoy platform.

**Definitions**

Software Platform – a system that holds collection of computer programs and can install, manage, and maintain the software.

Cybersecurity – The process of defending a particular software.

Authentication – The user must have a password and username to access the platform.

**Terms**

Saarikko, T., Jonsson, K., Burström, T. Explain that software platforms encompass a large amount of responsibility to ensure that there is a secure and manageable way to install software on computers. With the rapid development of cyber attacks that are happening, AppJoy has been developed with security first. Through continuous development and application monitoring, AppJoy will continue to develop and improve the AppJoy platform.

**References**

Huang, K., Siegel, M., & Madnick, S. (2018;2019;). Systematically understanding the cyber attack business: A survey. ACM Computing Surveys, 51(4), 1-36. <https://doi.org/10.1145/3199674>

Bossler, A. M. (2021). Neutralizing cyber attacks: Techniques of neutralization and willingness to commit cyber attacks. American Journal of Criminal Justice, 46(6), 911-934. <https://doi.org/10.1007/s12103-021-09654-5>

Saarikko, T., Jonsson, K., Burström, T., IT-fakulteten, Department of Applied Information Technology (GU), Göteborgs universitet, Gothenburg University, IT Faculty, & Institutionen för tillämpad informationsteknologi (GU). (2019). Software platform establishment: Effectuation and entrepreneurial awareness. Information Technology & People (West Linn, Or.), 32(3), 579-602. https://doi.org/10.1108/ITP-11-2016-0285

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees’ adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224. <https://doi.org/10.1016/j.im.2013.08.006>

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, 43, 90-110. https://doi.org/10.1016/j.cose.2014.03.004