Table of Contents

Table of Contents

Data Classification Policy

Clinton Connect collects data from its users to operate the platform and achieve the goal of preparing and deploying content to Connect PVMs, analyzing data relevant to the content displayed on the screen, and about the health and other statuses of the devices. This document categorizes the data we maintain and defines the amount of protection required for each category.

The data maintained in the Clinton Connect platform ("the platform") can be divided into the following categories:

- Public
- Internal
- Confidential
- Restricted

Public Data

Public data is information that is or may be made available to anyone. While it may not always be publicly available, it does not require any level of protection or access permission.

Public data available on the platform is limited to content produced by Clinton Electronics about the platform. This includes marketing materials, training materials, videos, and public policies such as the Privacy Policy and Terms of Use.

No data generated by users is considered public data, and will not be made available as such.

Internal Data

Internal data is private data maintained in the platform and considered potentially sensitive. It is not shared with the public. It includes information that will not be disclosed without the consent of the person or organization that created the data.

Most data generated by users and maintained by the platform falls into this category. It includes, but is not limited to: company/store information, media files uploaded to the platform, device information, analytics data, etc.

No internal data will be disclosed to outside parties without the permission of the person or organization which created the data.

Data Classification Policy Continued

Confidential Data

Confidential information is data is sensitive data, the disclosure of which would adversely affect individuals or organizations we do business with. As with Internal data, Confidential data will not be disclosed without the prior consent of the person or organization that created the data.

Additionally, Confidential data is not transmitted to third party systems that the platform may employ (such as media optimization services) or to the Connect PVMs. Confidential data is only available to privileged users within the platform.

Confidential data within the platform includes but is not limited to: user names/emails, order/subscription data.

Restricted Data

Restricted data is data that the platform is legally or contractually obligated to safeguard in the most stringent manner. Typically, this includes personally identifiable information, financial data, etc. The platform does not maintain any such data within our systems.

The one piece of data maintained currently by the platform is user account passwords. This data is never visible in plain text, nor is it stored in plain text. This data will never be disclosed and may only be used for account authentication. Users themselves are in charge of creating and changing this data.

Acceptable Use Policy

The Acceptable Use Policy defines the requirements for proper use of the Clinton Connect platform ("the platform"). The platform has been designed with the purpose of preparing and deploying content to Connect PVMs. Users of the platform have access to create and deploy content and view potentially sensitive information. Consequently, it is important that users behave in a responsible, ethical, and legal manner.

Scope

This policy applies to all users of the platform, which includes Administrators, Integrators, Company Owners, and any other users created by them within the platform. This policy also applies to the use of the web application and the Connect PVM devices, as well as any data stored in the platform.

Acceptable Usage

- You may only access the web application using the user account which you were assigned. You may not use another individual's account, or attempt to capture or guess other users' passwords.
- You are individually responsible for the use of all data available to you based on your role's permissions.
- You should make a reasonable effort to protect your passwords.
- You must not attempt to access restricted portions of the web application, platform, or any other system used by the platform.
- You must comply with all other policies and guidelines which govern the platform. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- You must not use the platform in conjunction with the execution of other programs, software, processes, or automated transaction-based commands that are intended to disrupt (or could be expected to disrupt) other users, or damage or degrade performance of the platform's software or hardware components.
- You must not use tools that are normally used to assess security or to attack software or hardware systems (ie. password crackers, vulnerability scanners, network sniffers, etc.) against the platform.

Fair Share of Resources

Clinton Electronics can be expected to maintain an acceptable level of performance and assure that inappropriate use of the platform by a few people does not degrade performance for others. However, the platform's resources must be utilized with consideration for others who also use them. Therefore, the use of any automated processes against the platform is forbidden.

Acceptable Use Policy Continued

Adherence with Federal, State, and Local Laws

- As a user of the platform, you are expected to uphold local, state, and federal laws.
- You must abide by any applicable copyright laws and licenses as they apply to image or video content used on the platform.
- Do not use copyrighted works unless you have a legal right to do so. Using such works without permission may provide the basis for account suspension, civil litigation, and criminal prosecution.

User Compliance

When you use the platform, you agree to comply with this and all other related policies. You have the responsibility to keep up to date on changes in the platform and its policies and to adapt to those changes as necessary.

Change Management Policy

The processes outlined in this policy define processes for making changes to the Clinton Connect platform ("the platform"). The goal of this policy is to increase awareness and understanding of how we make changes to the platform and ensure that all changes are made in a thoughtful way that minimizes a negative impact on services and customers.

Changes to the platform generally follow this process:

- Planning: this includes design, definition of requirements, scheduling, test planning, release planning, documentation, etc.
- Evaluation: this includes vetting the proposed change, determining risk, impact on existing systems and processes, updating documentation.
- Approval: obtain approval of the planned and evaluated change from stakeholders.
- Implementation: implementation and QA of the change.
- Review/Maintenance: Review the change and plan for future changes/improvements.

Scope

This policy applies to changes made to infrastructure, hardware, or software systems that make up the platform. Modifications to other systems such as development and QA processes, support systems, etc. do not apply to this policy.

Types of Change

- Maintenance Change: these changes happen on a regular schedule and include small pre-approved changes such as minor fixes or improvements. Maintenance changes may include portions of Feature changes but must have their functionality disabled by feature toggle.
- Feature Change: this is a change that represents a planned but potentially higher-impact change to the platform, such as a release of a new feature. In the case that this feature includes a feature toggle, this change may also include turning on this toggle. Management and software development teams must approve feature changes.
- Hotfix Change: this change is one that must be applied as soon as possible due to negative service impacts. There may be fewer people involved in the change management process due to the urgent nature of the issue, but these must still be approved by management.

Change Documentation

Release notes are produced for each Maintenance, Feature, and Hotfix change and may be provided upon request or posted publicly on the internet.

Incident Management Policy

The purpose of this policy is to outline the plan for properly handling and managing security incidents pertaining to the Clinton Connect platform ("the platform").

Incident Preparedness

Clinton Electronics remains prepared to respond to any incident in a timely manner. Our customer support team is trained and ready to respond to customer calls. Should extra training specific to the event be required, they will be prepared to respond to customer needs and requests. The customer support team will escalate any appropriate issues to the management or development team as necessary.

The development team will regularly monitor for incidents and breaches via software tools deployed on our servers. Any discoveries will be reported to the management team for incident response.

Incident Response

Once a security incident has been identified, the software development team will formulate a plan for containment and recovery. The management and customer support teams will begin communication with affected customers.

As soon as possible, after containing the incident and removing malicious code or unauthorized means of access, we will begin the data restoration process. Using backups, caches, etc. will restore information as closely as possible back to the point just before the incident.

Incident Review

Following all response and recovery, the management, development, and customer support teams will meet and review the events of the incident. They will discuss the causes and outcomes and make recommendations for improving our preparedness and response to guard against such an incident in the future.

Password Management Policy

Employee passwords are the first line of defense in securing the Clinton Connect platform ("the platform") from inappropriate or malicious access to data and services. Regardless of whether accounts are used for workstation, development tool, platform, or service access, the following policy will be employed for password management.

- Many of our workstation computers are equipped with fingerprint readers for access. These should be used whenever possible.
- Employees will use a password manager supplied by Clinton Electronics for generating and maintaining the passwords used for various accounts.
- When an account requires a password, employees will supply one generated by the password manager and save that password in that password manager for later use.
- When it is not possible to use the password manager to maintain a password (i.e. for workstation account access), employees will adhere to current accepted strong password creation policies.
- Employees will generate and store a different password for each account that they use.
- Passwords should never be written down or stored outside of the password manager for any reason.
- Whenever possible, employees will enable two-factor authentication for their user account.

Encryption Policy

Encryption offers a means of protecting data in transit or stored on devices. This policy outlines recommended encryption technologies for use on the Clinton Connect platform ("the platform"). Ciphers that are proven, standard, and highly tested must be used as the basis for encrypting data.

Encryption At Rest

When data such as databases ad files encrypted at rest, it should be encrypted using AES-256 or Triple-DES. Keys used for this encryption should be at least 256-bits in length. Any private or confidential information should be encrypted at rest.

Encryption In Transit

All data transmitted as part of the platform will be encrypted. This encryption should be done using industry-standard SSL/TSL 1.1 or 1.2 and use a 2048 bit RSA signature.

Hashing

For the purposes of the platform, hashes may be used as a means of obfuscating data. Hashing may be used when the data in its raw format is not required. Hashing should not be considered a form of encryption. Various hashing algorithms may be used depending on their use case. For instance, passwords may be hashed using Bcrypt but not MD5. MD5 may be used to hash a file's contents in order to compare.

Data Retention Policy

This policy outlines data retention practices for the Clinton Connect platform ("the platform"). The purpose of this policy is to minimize the retention period of records while ensuring that the business needs of our customers are met.

Scope

This document applies to the retention of personal data, which is retained as part of the platform. This includes but is not limited to account data, email addresses, media files, and other data collected by the platform.

Policy

Personal data shall not be kept for longer than is necessary for a given purpose. However, the retention period can differ based on the type of data processed. Currently, we maintain our backups at the following schedule:

- Daily backups are maintained for 16 days.
- Weekly backups are maintained for 8 weeks.
- Monthly backups are maintained for 4 months.
- Yearly backups are maintained for 2 years.

After the retention period has expired, the personal data does not necessarily have to be completely erased. It may be anonymized. In cases where the data cannot be allocated to an identifiable person, no action will be required.

Privacy Policy

Clinton Electronics ("us," "we," or "our") operates the https://app.clintonconnect.com website (the "Service").

This page informs you of our policies regarding the collection, use, and disclosure of personal data when you use our Service and the choices you have associated with that data.

We use your data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, terms used in this Privacy Policy have the same meanings as in our Terms and Conditions, accessible from https://app.clintonconnect.com.

Information Collection And Use

We collect several different types of information for various purposes to provide and improve our Service to you.

Types of Data Collected:

Personal Data

While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personally identifiable information may include, but is not limited to:

- Email address
- First name and last name
- Phone number
- Address, State, Province, ZIP/Postal code, City
- Cookies and Usage Data

Usage Data

We may also collect information about how the Service is accessed and used ("Usage Data"). This Usage Data may include information such as your computer's Internet Protocol address (e.g., IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

Privacy Policy Continued

Tracking & Cookies Data

We use cookies and similar tracking technologies to track the activity on our Service and hold certain information.

Cookies are files with a small amount of data, which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyze our Service.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

Examples of Cookies we use

- Session Cookies. We use Session Cookies to operate our Service.
- Preference Cookies. We use Preference Cookies to remember your preferences and various settings.
- Security Cookies. We use Security Cookies for security purposes.

Use of Data

Clinton Electronics uses the collected data for various purposes:

- To provide and maintain the Service
- To notify you about changes to our Service
- To allow you to participate in interactive features of our Service when you choose to do so
- To provide customer care and support
- To provide analysis or valuable information so that we can improve the Service
- To monitor the usage of the Service
- To detect, prevent and address technical issues

Transfer of Data

Your information, including Personal Data, may be transferred to — and maintained on — computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

If you are located outside the United States and choose to provide information to us, please note that we transfer the data, including Personal Data, to the United States and process it there.

Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

Privacy Policy Continued

Clinton Electronics will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

Disclosure of Data Legal Requirements

Clinton Electronics may disclose your Personal Data in the good faith belief that such action is necessary to:

- To comply with a legal obligation
- To protect and defend the rights or property of Clinton Electronics
- To prevent or investigate possible wrongdoing in connection with the Service
- To protect the personal safety of users of the Service or the public
- To protect against legal liability

Security of Data

The security of your data is important to us, but remember that no method of transmission over the Internet or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

Service Providers

We may employ third party companies and individuals to facilitate our Service ("Service Providers"), to provide the Service on our behalf, to perform Service-related services or to assist us in analyzing how our Service is used.

These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

Links To Other Sites

Our Service may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies, or practices of any third party sites or services.

Privacy Policy Continued

Children's Privacy

Our Service does not address anyone under the age of 18 ("Children").

We do not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or guardian and you are aware that your Children has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

Changes To This Privacy Policy

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update the "effective date" at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted to our online Privacy Policy page.

Platform Security

This document gives an overview of the Clinton Connect security strategy across the entire platform. Currently, the platform consists of three components: the Server, Web Client, and the Connect Public View Monitor (PVM). While developing the Clinton Connect platform, we have taken steps to ensure the security of each of these components individually and as a whole. That commitment to the security of your data continues as the platform grows. Below is a brief introduction to each of the platform components.

Server

The Server is the backbone of the Clinton Connect platform. Both the Web Client and the PVM Client communicate with the Server to be able to process the information they need to do each of their individual jobs. The Server handles network requests, communications with third-party services, business logic, and data storage.

Web Client

The Web Client is the portal that Clinton Connect users use to access and manipulate their data. The web client is accessible via a web browser at https://app.clintonconnect.com. All functionality of the Clinton Connect platform is initiated through the Web Client. For example, Company Users may log in to upload media, create advertisements, and deploy schedules. Company Owners may log in to manage access to their company's data. Integrators may log in to create a new Company and prepare for PVM installations across that Company's stores.

Connect PVM

The Connect PVM consists of both the hardware PVM itself as well as the software which runs it. The Connect PVM is in many ways like a traditional PVM. It uses a camera to display a live video feed on its screen, providing a theft deterrent. However— the Connect PVM also employs an on-board computer that can download media and display advertising on the screen, making it part of the Clinton Connect platform.

Security Strategy

The security strategy of the Clinton Connect platform is a multi-layered strategy that includes both software and hardware considerations. Precautions take into account both accidental and malicious incidents. Below we will describe specific steps we have taken regarding potential vulnerabilities and how they apply to each of the platform components.

Platform Security Continued

Network Communications

All data on the Clinton Connect platform is encrypted while in transit. This means that all data sent between the Server and Web Client, Connect PVM and Server, and between the Server and any third-party services remains encrypted via industry-standard SSL technology (HTTPS). The Web Client and Connect PVM only require a connection to our Server, push notification service, and our file server. Network admins may easily limit traffic on their network to these three sources - making their network even more secure. In the case of high network load, or a network-based attack such as a Distributed Denial of Service (DDoS), we employ a load balancer and request rate limits to keep the application running. We can ban traffic from offending IP addresses if needed.

Identity Protection

All access to the Clinton Connect platform (specifically, access to the Server via the Web Client) requires a login by username and password. It is a closed ecosystem in that users may not self-enroll. A user may only be issued account access by a privileged user. We employ a tiered Access Control List based on Roles and Permissions to prevent people from accessing and manipulating sensitive data. For example, users must have sufficient permissions to deploy a schedule to potentially thousands of devices. Other permissions are required for setting up new companies and users.

Two-Factor Authentication (2FA) has become a standard way for users to add an extra layer of Identity Protection. 2FA increases security by requiring not only something a user knows (their password) but also something they possess (typically their phone) to gain access to their account. Once a user enters their correct password, they must also provide a code which is either sent to or generated by their phone. 2FA is only available by request and will require a third party "authenticator service," such as Google Authenticator or Authy.

While the Connect PVMs are not technically users, they do connect to the Clinton Connect platform and therefore must be authenticated. Each Connect PVM receives an access token during installation, and all access to the Server via the Connect PVM is protected by authentication via an access token.

Data Storage

Data stored in the Clinton Connect platform is protected against loss. Database backups are made nightly and stored for an extended period. Most data is never deleted immediately, only marked for deletion at a later date. This way, we can easily restore items "accidentally" deleted by any user. The Web Client and the Connect PVM are both designed as "thin clients," meaning they store very little data locally, and any data can easily be restored to them from the Server.

All files stored in Clinton Connect (such as images and videos used for advertisements) are stored on servers designed for mission-critical primary data storage. It is a highly-redundant environment capable of sustaining the concurrent loss of two data centers and offering a 99.99% availability.

Platform Security Continued

Physical/Hardware Security

While many security precautions are software-related, potential vulnerabilities have been addressed on a physical/hardware level as well. Clinton Connect uses hardware owned by various third-party services for computing power, data storage, and file storage. These services are chosen in part because of their commitment to the security of their clients. We use only world-class, enterprise-level service providers who are among the top ten such service providers in the world.

Among their touted physical security features are the following:

- A globally-redundant infrastructure
- 24/7 physical security guard services
- CCTV coverage externally and internally for the facility
- Biometric readers with two-factor authentication
- Battery and generator backup

The Connect PVM itself has been designed with security in mind. All Connect PVMs are constructed with a ruggedized steel case with an acrylic vandal-resistant face. Access to all physical access ports (USB, Ethernet, etc.) is protected behind a steel panel held in place with a vandal-resistant Torx screw.

Summary

Clinton Electronics takes the security of your data very seriously. We have designed the Clinton Connect platform from the ground up with security in mind. Be it software or hardware solutions, preventing accidental loss or malicious attacks, we are committed to providing a platform you can trust. This commitment continues as we continually improve the security of the platform.

Network Architecture

Clinton Connect Networking

The Clinton Connect platform is a secure, cloud-based network designed to allow users to manage the deployment of advertising materials to thousands of devices from anywhere in the world. The cloud-based architecture alleviates the hassles of installation, setup, and network management as there is no port-forwarding or static IP address required. This also makes the platform more secure. No open or forwarded ports means less exposure to potential attackers. All connections between Clinton Connect devices are encrypted, and communication is restricted to our servers only.

To understand the basics of the network architecture, we'll need to explain the three essential pieces: the Connect Web Client, the Connect PVM, and the Connect Cloud Services.

Connect Web Client

The web client is a browser-based web application accessed via https://app.clintonconnect.com. Through a password-protected portal, users may manage devices, upload media, and create and deploy ads to their devices. The web client connects via an encrypted connection directly to the Connect Cloud Services in order to do so. This involves communicating with our Virtual Private Cloud servers, downloading content from our Content Delivery Network (CDN), and receiving real-time messages from our Real-time Messaging service.

Connect PVM

The connect PVM is the most visible piece of the platform, as there may be thousands of connected devices receiving content to display on their screen for customers to see. Devices establish an internet connection during an on-boarding process where it will be connected to a network either by ethernet or wifi. As long as the device can reach the internet (and specifically our servers), that is all the network setup required.

When a user deploys content to a device via the Connect Web Client, our Connect Cloud Services sends a notification to the PVM to alert it that new content is available. At that time, the PVM connects securely to the CDN to download the needed content and display it on the screen.

Apart from deploying content, users may also manipulate certain aspects of the PVM remotely via the web client. For example, LED settings and volume can be controlled remotely, and the device can be rebooted remotely. Similarly to the deployment process, these changes are pushed from our Connect Cloud Services out to the devices.

Network Architecture Continued

Connect Cloud Services

As you can tell, the Connect Cloud Services play a central part in network architecture. All network communications flow in and out of our cloud services. The cloud services consist of three parts: Virtual Private Cloud, Cloud Storage/CDN, and Real-time Messaging. The Virtual Private Cloud handles all incoming communications from both the web client and PVM. It handles incoming files and places them in Cloud Storage. The CDN handles serving files both to the web client and PVM. Lastly, Realtime Messaging responsible for direct communication from Connect Cloud Services out to Connect Web Clients and PVMs. As these are mission-critical to our platform, all Connect Cloud Services employ multiple redundancies, and all communications in, out, and between services are encrypted.

Network Diagram