Collectrium Security White Paper

Version 2.5

January 2018

The policies, procedures and technologies described in this paper are accurate at the time of publication. Specifics may change over time, as Collectrium is committed to innovation. Updates to this document will incorporate reference to any impact of new features released onto the platform. The latest version of this paper can be found at http://www.collectrium.com/security.

Table of Contents

Introduction

Thousands of collectors and art professionals trust Collectrium to store and share their collection management data and files simply and privately. This security white paper details the security infrastructure and configuration Collectrium uses to protect data and assets entered into the platform. The white paper also covers specific security and privacy topics that may be of concern to existing and potential Collectrium clients, such as how the data is stored, additional user permissions on an account and secure access from a mobile device.

The paper is written for collection owners, managers and security personnel, and assumes that you are familiar with basic security concepts. Links to external resources are supplied in places in this document, for those who would like more information on the concepts referenced.

Overview

Collectrium offers thousands of collectors around the world a secure web platform to manage their high-value fine art and collectibles. Subscribers can access their collection-related data from any Internet-capable device. The cloud environment allows unlimited storage capacity and mobility.

Every component of the Collectrium cloud-based infrastructure, including compartmentalization, server assignment, data storage and processing, is focused on security and privacy. No one can view your information on Collectrium but you as the Account Owner, and any users you nominate. Everything you enter is encrypted and stored at data centers with bank-level security, keeping it private and confidential no matter where you're accessing it from.

This document will explain how Collectrium creates a secure and private platform, detailing topics in four key areas: Confidentiality Processes, Application Security, Data Security and Infrastructure Security.

1. Confidentiality Processes

1.1. Industry-Leading Privacy Policy

Our Privacy Policy gives users complete control of the data they entrust to Collectrium. To guarantee complete privacy and security to our users, we designed our Privacy Policy to reflect a conservative interpretation of industry best practices.

The current Collectrium Terms of Service and Privacy Policy can be reviewed at http://www.collectrium.com/terms-of-services/
and http://www.collectrium.com/privacy-policy/.

1.2. No Data Access by Collectrium

Collectrium employees, including software engineers and application developers, do not have access to client data.

Server Management

We do not outsource server management or any management that would give third parties access to customer data. The technical employees who maintain the servers are carefully selected and screened. Each expert has a minimum of ten years' professional experience and undergoes an extensive background check before being hired.

Security Training

The technical employees who maintain Collectrium servers undergo in-house security training in order to guarantee the expected level of total confidentiality and security for all data entered into the platform.

Client Support

In cases when the Account Owner requests support services from Collectrium, support personnel must receive explicit permission from the Account Owner to access the account. To grant access, the Account Owner must go to the Settings area of their Collectrium account and explicitly grant Collectrium support personnel account access.

Collection Data Import

During the process when the Collectrium support team assists the Account Owner in correctly importing their collection data onto the Collectrium platform,the Account Owner's data is securely stored and accessible only by the support team. Once the transfer process is complete, all documents pertaining to the Account Owner's collection are permanently deleted and the Account Owner receives official notice of the event.

1.3. No Data Access by Christie’s Group Companies

Collectrium, Inc. is a member of the Christie’s group of companies and is independently operated with its own management, employees and business infrastructure. There is no data sharing between Collectrium and any other Christie’s Group Company in either direction. Collectrium and Christie’s group of companies do not share data centers.

Collectrium will not share your personal information or collection with a Christie’s Group Company without your explicit consent. If you are considering sharing your information with a Christie’s Group Company, we encourage you to review their privacy policy first.

1.4. Employee Background Checks

All Collectrium employees are carefully selected among the experts in their fields and undergo extensive background checks before hire. All job offers are contingent upon the employee’s satisfactory completion of extensive background and drug tests.

1.5. Security Audits

In order to validate that the practices outlined in this document are up-to-date and industry-standard, Collectrium security processes are regularly audited by a Big Four global auditing firm – most recently, by Deloitte. Collectrium is also regularly audited by potential partner companies looking to integrate their services with Collectrium.

2. Application Security

2.1. Proven, Secure Coding Practices

The Collectrium Platform is developed following Open Web Applications Security Project (OWASP) Secure Coding Practices. OWASP is a global non-profit devoted to researching and publishing the most up-to-date and secure methods of developing software.

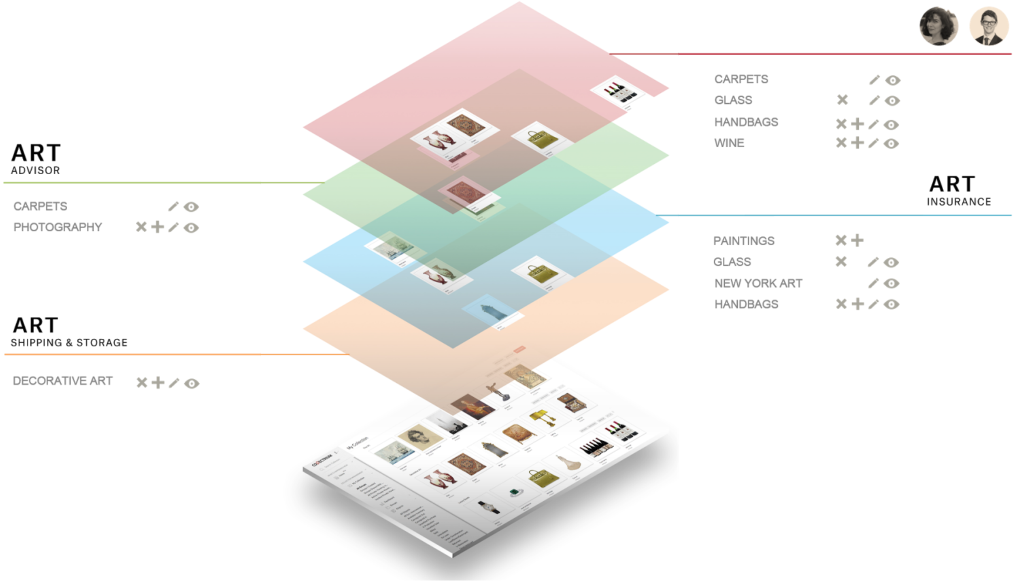
2.2. Secure Connections

All connections to Collectrium servers are through Hypertext Transfer Protocol Secure (HTTPS). HTTP is the protocol over which data is sent between your web browser and the majority of websites and apps on the Internet. The HTTPS protocol adds security by encrypting your data while it is being transferred, through the use of TLS 1.2 protocols. TLS 1.2 is the global standard for encrypting Internet data transfers.

2.3. Account Access Permissions

Roles within a Collectrium Account

The Account Owner may create additional users within the account, specifying the role and level of access for each of these users. These granular privacy settings are fully customizable so that each user's access is limited to precisely the data areas, functionality and actions that the Account Owner specifies, affording optimum privacy and control.



2.4. Multi-Factor Authentication

This option is available for all users of Collectrium. When configured and enabled, successful account access can only occur if the user provides a username, password, and one-time use code sent by SMS at the time of sign-in.

2.5. Private Viewing Rooms

This is a private, visual digital space which gives the Account Owner the ability to grant a third party *temporary* access to specific objects and select details, for example to request a shipping or insurance quote from a Collectrium partner. The Account Owner may revoke access to a Private Viewing Room at any time.

2.6. Collectrium Supported Browsers

We currently support the following web browsers:

- Chrome v31+ on iOS, Android, OS X, Linux, Windows
- Safari v7+ on iOS, OS X
- Opera v20+ on iOS, Android, OS X, Linux, Windows
- Firefox v27 on iOS, Android, OS X, Linux, Windows, Firefox OS
- Internet Explorer v11+ on Windows

Earlier versions of these browsers do not support TLS 1.2 security, which may put a subscriber's data at risk. Collectrium therefore recommends use of one of the above supported browsers only.

2.7. Mobile Platform Security

iOS

Collectrium offers an iOS app for your Apple iPhone or iPad, which can be found in the iOS App Store. The Collectrium iOS app is supported on iOS 8.0 or higher, which can currently be installed on iPhone models 4S and newer and iPad models 2nd generation and newer. Security features include:

- Data encryption at the iOS file system level: files are accessible only when the iPhone/iPad is unlocked with the correct passcode.
- Certificate pinning within the application: the Collectrium server sends a certificate, which is unique identifying information, with every transmission that it makes. Certificate pinning is the practice of storing a list of trusted certificates within the app and then validating the server certificate against this trusted list. If the data is not valid, the data transfer does not happen. In this way, the app ensures communication happens only with the Collectrium server.
- Jailbreak and debugger detection at runtime:
  - Jailbreaking is the process of removing software restrictions from a device's operating system, in this case iOS for iPhone and iPad. In many cases, these are restrictions which are imperative for a secure device. The Collectrium app operates with the expectation that iOS is operating as securely as it should. If jailbreaking is detected, the Collectrium app will not work, in order to keep your data secure.
  - A debugger is a program that is typically used when writing computer code. It allows the programmer to detect and correct errors in code. Unfortunately, debuggers can be used

maliciously to reverse engineer code, creating a potential security risk. Before starting, the Collectrium app checks for debuggers and will operate only if none are detected.

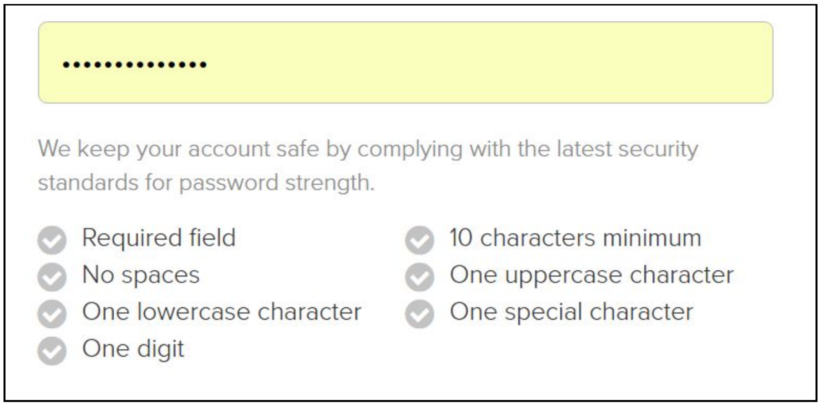
2.8. Password Requirements

In order to ensure the highest level of security for our users, Collectrium follows OWASP recommendations concerning password creation as a strong password greatly reduces the likelihood that a human or computer could intelligently guess a password, thus granting them unauthorized access to an account.

This is why all new users are required to select a strong password to access their Collectrium account. The requirements for valid passwords are:

- 10 characters minimum
- No spaces
- Include one uppercase character
- Include one lowercase character
- Include one digit
- Include one special character

Help is provided to the users at sign up to construct a secure password:



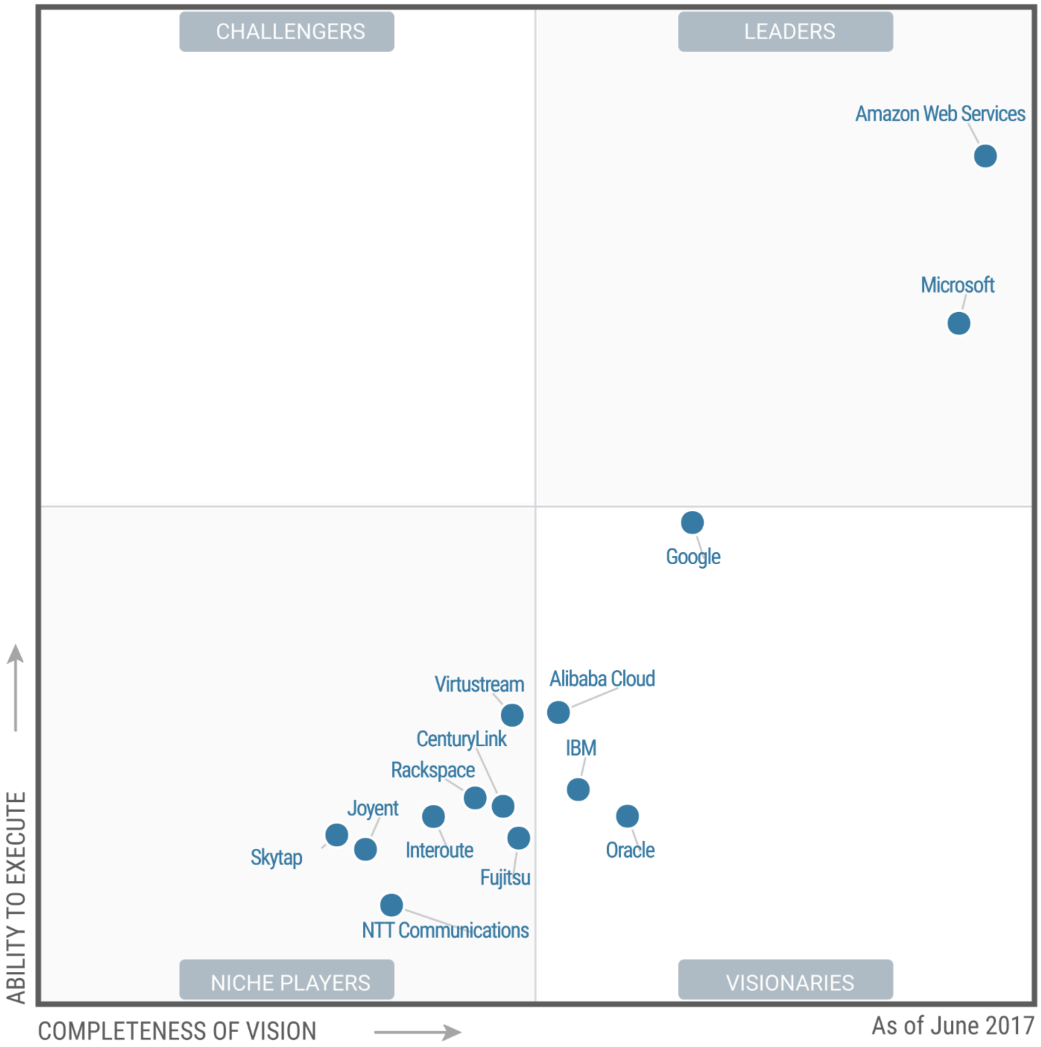
•••••••••••••••

We keep your account safe by complying with the latest security standards for password strength.

- ✓ Required field
- ✓ No spaces
- ✓ One lowercase character
- ✓ One digit
- ✓ 10 characters minimum
- ✓ One uppercase character
- ✓ One special character

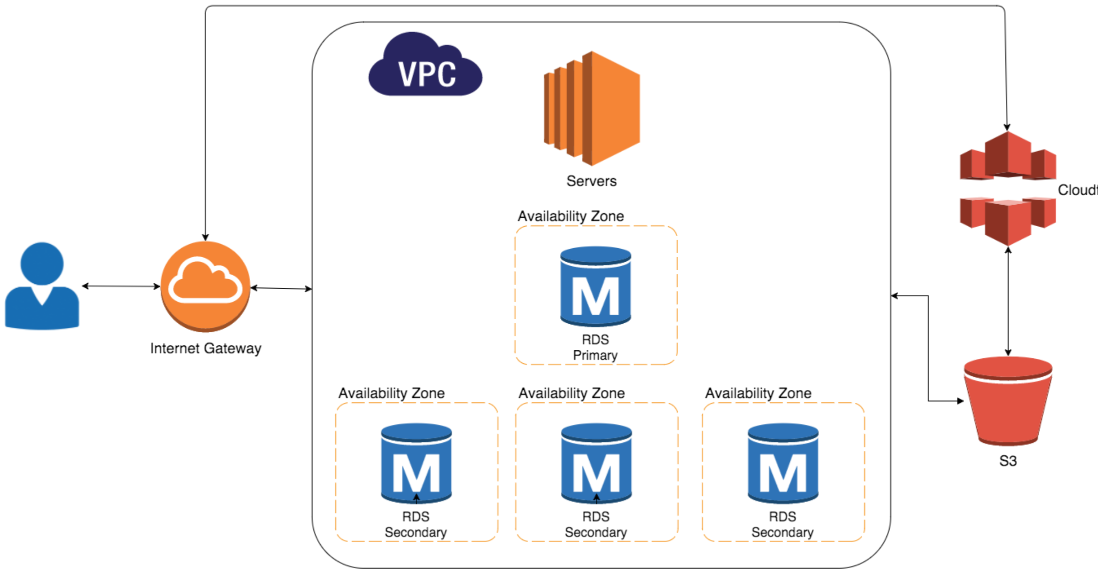
3. Data Security

Collectrium uses Amazon Web Services (AWS) to host the Collectrium platform and its supporting infrastructure. AWS is currently the industry leader in cloud infrastructure security, as reported by Gartner in the 2016 Magic Quadrant for Cloud Infrastructure as a Service, Worldwide Report.



3.1. Data Storage

Collectrium data is stored using Amazon Web Services (AWS) Relational Database Service (RDS). Multi-availability zone architecture and automated backups greatly increase durability. This database and the Collectrium servers reside within an AWS Virtual Private Cloud (VPC), which is a virtual network owned, controlled and configured by Collectrium. Asset storage (files, images, etc.) utilizes AWS Simple Storage Service (S3) which offers durability of 99.999999999% and redundant storage across multiple facilities.



3.2. Data Backup

Automated backups of our RDS database occur once a day. We retain each backup for the maximum number of days allowed by Amazon, safeguarding against the loss of your information while guaranteeing data will not be stored any longer than necessary. Complete copies of the database are stored in different availability zones. These are different physical locations, a minimum designated distance apart, each with independent support systems. This means that if one instance of the database goes down because of an outside occurrence (extreme weather, for example), the database at the next location goes up, and is a sufficient distance away not to be affected by the same issue, thus guaranteeing continuous operation. Use of multi-zone architecture provides another level of safeguarding. In the unlikely event that the primary database fails, AWS automatically switches to the backup database, and this backup includes the entire database.

3.3. Data Removal Upon Deletion of Account

All data is deleted from the Collectrium database upon receipt of a request from the Account Owner. Collectrium has a secure process in place for any requests of this nature. We will not restore an account once it has been deleted.

3.4. No On-Site Storage of Data

Absolutely no data is stored on site at any Collectrium office. Please see Data Storage for further information.

4. Infrastructure Security

4.1. Penetration Testing

The Collectrium platform is subject to regularly scheduled rounds of penetration testing. The purpose of this testing is to search a network or web platform for security vulnerabilities that a malicious third party might exploit. Our latest round of penetration testing was done by NCC Group, a global information assurance specialist with security expertise, known for its comprehensive approach to helping thousands of organizations around the world ensure proper management of risk and threat limitation.

4.2. Secure Access

System Administrators connect to all AWS services using secure HTTPS/TLS 1.2 connections.

4.3. Key Management

Permission keys used by Collectrium System Administrators to access or modify AWS are managed in a highly secure fashion. Keys are never shared over a digital network and are only stored on encrypted devices which meet United States government security standards.

4.4. Unique AWS Users

Identity and Access Management is a service offered by AWS that is used to control the level of access users have to AWS. Developer access to AWS is logged and monitored.

4.5. AWS Firewalls

All AWS databases and servers reside within an AWS Virtual Private Cloud (VPC), which is a virtual network owned, controlled and configured by Collectrium. Outside access to the VPC is through an Internet Gateway. This firewall allows Collectrium to control and monitor who can access its servers. Images, documents and other assets that are stored using AWS S3 are securely accessed and served directly from the firewall-protected VPC or using the AWS Cloudfront service, which is a global content delivery network that transfers encrypted asset data to your device from the nearest AWS S3 data center.

4.6. Encrypted Data Storage

Collectrium data and assets stored in AWS S3 are automatically encrypted using Advanced Encryption Standard (AES) 256 encryption.

4.7. Data Center Compliance

All AWS data centers are compliant with multiple audit and review protocols. These include:

- SOC 1
    - A Service Organization’s Control 1 (SOC 1) is a report on controls which are relevant to user entities’ internal control over financial reporting.

- SSAE 16/ISAE 3402 (formerly SAS 70)
    - Statement on Standards for Attestation Engagements 16 (SSAE16) is an American Institute of Certified Public Accountants (AICPA) auditing standard intended to provide customers and prospective customers with third-party validated visibility of a service provider's controls. SSAE 16 is an American standard consistent with the international standard, ISAE 3402.

- SOC 2 Type 2
    - A Service Organization's Control 2 (SOC 2) Type 2 is an additional report specifically designed for organizations such as software as a service (SaaS) vendors, data centers and other technology and cloud computing-based businesses. A Type 2 report includes the auditor's opinion on whether the service's internal controls are operating effectively and describes the test of the controls performed by the auditor to form that opinion.
- SOC 3
    - A Service Organization's Control 3 (SOC 3) is an additional report which outlines information related to a service organization's internal controls for security, availability, processing integrity, confidentiality and privacy.
- FIPS 140-2
    - The Federal Information Processing Standard Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to accredit cryptographic modules.

- MTCS Level 3
    - The Multi-Tier Cloud Security (MTCS) is an operational Singapore security management Standard (SPRING SS 584:2013), based on ISO 27001/02 Information Security Management System (ISMS) standards.

4.8. Payment Platform Compliance

Our payment platform is industry standard, PCI-DSS Level 1 compliant. The Payment Card Industry Data Security Standard (PCI-DSS) is administered and managed by the Payment Card Industry Security Standards Council (PCI-SCC), an independent body created jointly by the major credit card brands. The PCI-DSS is a set of requirements designed to ensure that all companies which process, store or transmit credit card information maintain a secure environment.

4.9. Physical Security Measures

AWS Facilities

All AWS data centers are built with robust physical security. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled, both at the perimeter and at building ingress points, by professional security staff utilizing video surveillance, intrusion detection systems and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification, and are signed in and continually escorted by authorized staff. AWS provides data center access and information only to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, access is immediately revoked, even if he or she continues to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Collectrium Facility

The Collectrium offices are locked at all times. Employees gain access with an electronic photo identification keycard. Visitors and contractors must check in before they are granted access, and they are monitored for the duration of their stay. As stated above, Collectrium data and client data are never stored on site in any Collectrium offices, to prevent theft of physical systems that contain confidential information.

All employees adhere to a strict “No-Print” policy concerning private information. Should private information be printed erroneously, paper shredders are located next to all printers and will be utilized immediately.

4.10. Disaster Recovery

All digital information is stored using AWS. The multi-zone architecture of our AWS ensures that data is backed up and served from multiple locations. These layers of redundancy are built into the infrastructure to greatly reduce the possibility of data loss. This is described in more detail in the Data Backup section.

4.11. Documented Incident Response Policy

Collectrium has a Documented Incident Response Policy that outlines a clear, efficient method for responding to possible digital security risks.

Conclusion

Collectrium offers peace of mind to collectors of high-value fine art and collectibles, who are concerned with the security and privacy of their assets. We provide a carefully designed set of security services and privacy features to give our clients the utmost assurance that the data relating to their assets is stored and managed in the most secure manner possible.

Using the latest industry best practices highlighted in this white paper and always keeping up to date with the highest security standards and upgrades, we ensure that Collectrium continues to offer industry-leading security and privacy to its users.