PitchVantage Security Policy and Guidelines

Purpose

This document addresses how user data is processed, handled, accessed and stored securely by PitchVantage. It also informs about IT and hardware requirements to access PitchVantage.

Hosting and IT Infrastructure

PitchVantage uses AWS (Amazon web services) servers to process and store data. AWS is one of the most trusted service providers by millions of the organizations for their IT Infrastructure. Amazon's infrastructure has a high-level security and availability that provides companies' ability to deploy a resilient IT architecture. AWS has designed its systems to tolerate hardware failures with minimal customer impact.

AWS has implemented a world-class network infrastructure that is carefully monitored and managed. AWS network has firewalls, employ rule sets, access control lists (ACL) and traffic flow policies to manage and enforce the flow of traffic. ACL policies are approved by Amazon Information Security.

AWS allows you to establish a secure communication session with your storage or compute instances within AWS. In addition, AWS has implemented network devices that are dedicated to managing communications with Internet service providers (ISPs). Some more information on security practices:

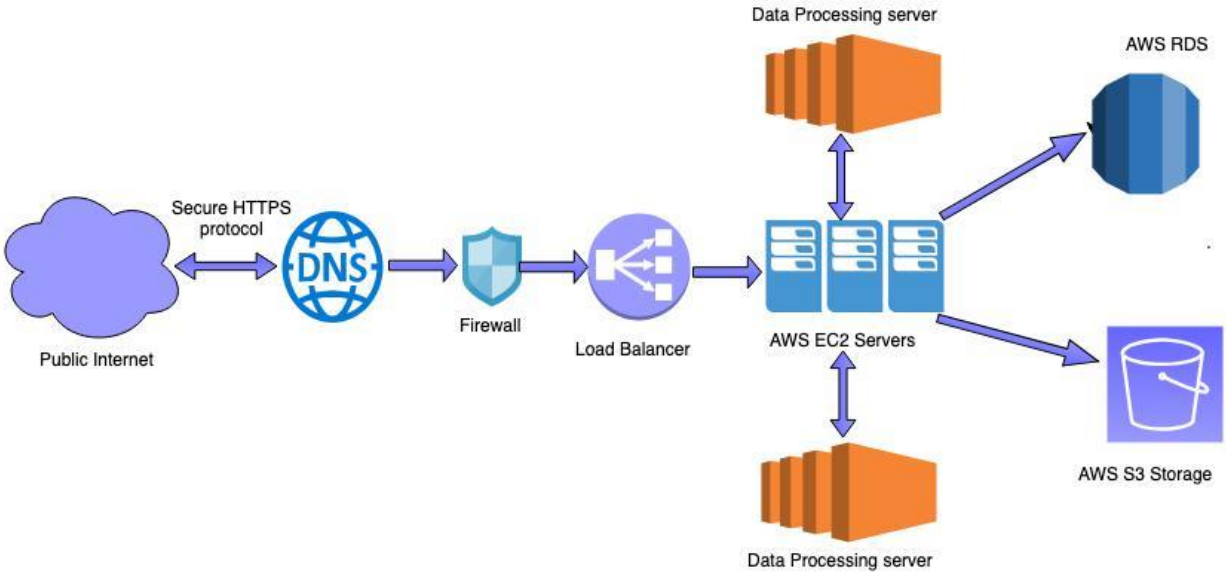
1. Security Process
2. Compliance
3. Certification

Data Storage and Access Policy

1. Personal info (except audio & video) in Amazon Web Services (AWS) RDS servers in the US.
2. Audio and Video files are stored on AWS S3 servers in the US
3. Log file are stored on EC2 Servers in the US.

User's voice data is analyzed to provide PitchVantage scores. All data is subsequently stored on AWS servers and accessible to user, approved user's organization administrators and PitchVantage employees who need to know. Need to know employees require Multi-factor Authentication to access information and are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.
All audio/video files are stored on AWS S3 servers and can be access via signed links, which will be active only for limited amount of time.

Data transfer Protocol: All the data transferred over secure protocol via HTTPS.
User passwords are encrypted.



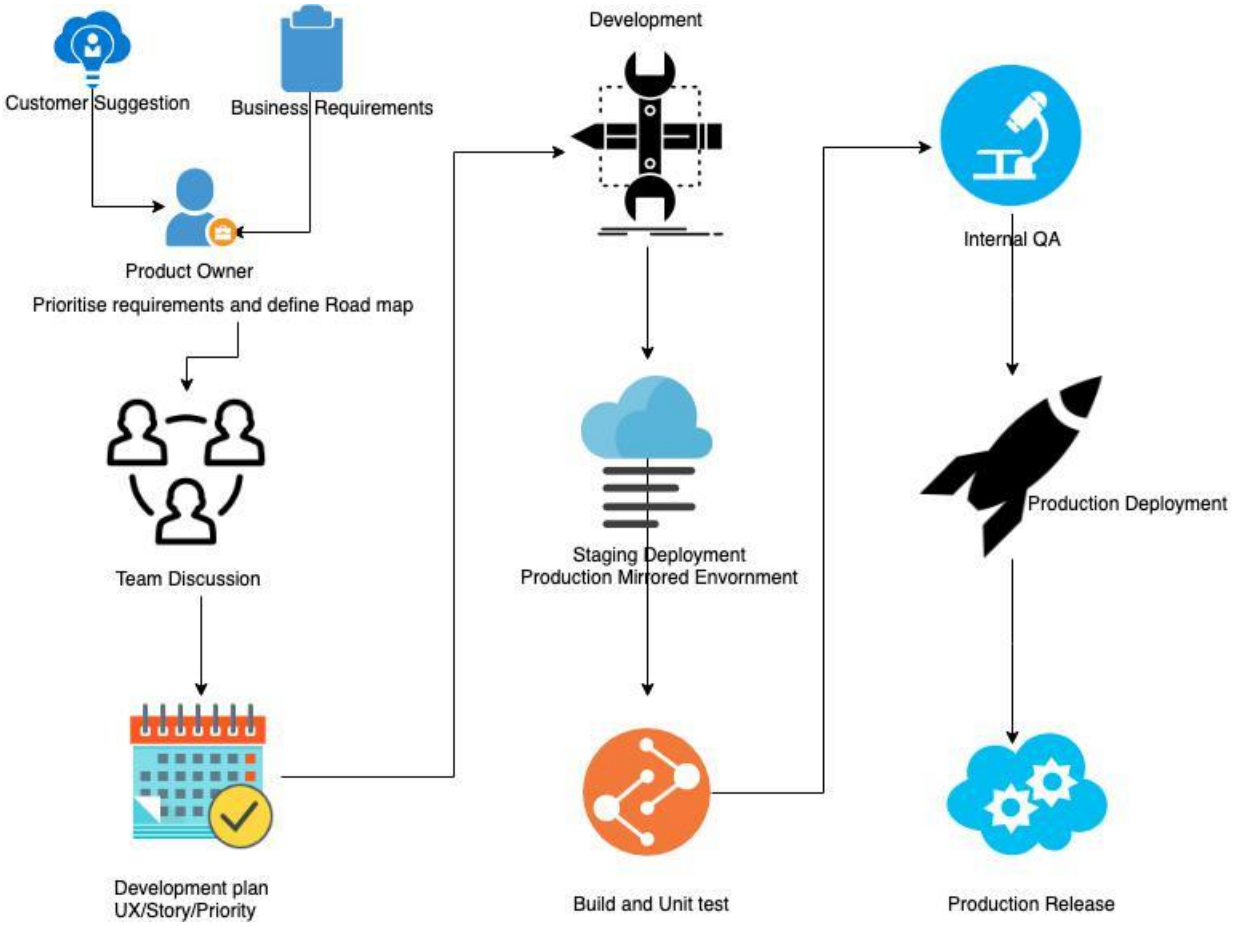
If user chooses to get scores on their content, we explicitly ask user consent before doing so. To transcribe user's presentation, user's audio file is transferred to Google Cloud. Audio file is saved in google bucket transcribed via Google Speech Api and data sent in JSON format back to PitchVantage AWS servers. On successful data transfer back to our servers, data in Google Bucket is deleted automatically. We do not log any data on Google cloud. Some more information on Google Cloud security policy:
https://cloud.google.com/security/overview/whitepaper
https://cloud.google.com/speech-to-text/docs/data-logging#data-security

PitchVantage Development and Quality Control

PitchVantage ensures production environment is scalable and available by following industry best practices.

PitchVantage's in-house development team uses Github for source code storage and only authorized users can access it via multi-factor authentication.

PitchVantage uses staging environment for all the local development and testing to ensure stable production environment. PitchVantage follows Agile Software development using Kanban framework and use Jira for tracking issues. PitchVantage has both manual and automated QA cycles to verify function, logic and integrity test before any feature release. We conduct standard and exploratory testing cycles and associated bug fixes on multiple devices before a release to production and only authorized personnel can perform a release to production environment.



Data Protection

PitchVantage stores all user information on AWS RDS that is secure and can be accessed only via AWS hosted server. No direct connection can be made to DB and its protected via network ACL.

All videos are stored on AWS S3 buckets with strict controls to bucket access with deletion protection. Videos can be accessed by users via PitchVantage application or PitchVantage online dashboard after user authentication. User's video data can be seen only by the user, unless they choose to share it with their organization's administrator. We ask for explicit consent from the user before doing so. All video data viewed by users and their administrators on the cloud have pre-Signed URLs that expire after a fixed time and prevents video to be downloaded for additional security. PitchVantage uses AWS suggested best practices including a firewall to control access.
Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt user data.

Backups. PitchVantage secures backups of all data in the following manner:

- Incremental backups of all uploaded media on multiple back-up servers (daily).
- Full backups of the database (daily, retention of 7 days).

In the (unlikely) event of damage or outage, PitchVantage will restore Customer's data from the most recent backup. This will be treated as a High priority issue.

PitchVantage Privacy Policy: https://cp.pitchvantage.com/pages/privacy-policy.html
PitchVantage Use Policy: https://cp.pitchvantage.com/pages/terms-of-use.html

Password Policy and Guidelines

Policy Statement

All individuals are responsible for safeguarding their PitchVantage credentials and must comply with the password parameters and standards identified in this policy. Passwords must meet the complexity requirements outlined and must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.

Reason for Policy

Assigning unique user logins and requiring password protection is one of the primary safeguards employed to restrict access to user's PitchVantage accounts. If a password is compromised, access to information systems can be obtained by an unauthorized individual, either inadvertently or maliciously. Individuals with PitchVantage accounts are responsible for safeguarding against unauthorized access to their account, and as such, must conform to this policy in order to ensure passwords are kept confidential and are designed to be complex and difficult to breach. The parameters in this policy are designed to comply with legal and regulatory standards, including but not limited to Payment Card Industry Data Security Standard (PCI DSS).

Individual Responsibilities

Individuals are responsible for keeping passwords secure and confidential. As such, the following principles must be adhered to for creating and safeguarding passwords:

- Passwords must never be shared with another individual for any reason or in any manner not consistent with this policy. A shared or compromised PitchVantage password is a reportable security incident.
- PitchVantage Employees as well as PitchVantage users, must never ask anyone else for their password. If you are asked to provide your password to an individual or sign into a system and provide access to someone else under your login, you are obligated to report this to PitchVantage support.
- Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.

Responsibilities of Systems Processing Passwords

All PitchVantage systems—including servers, applications, and websites that are hosted by or for PitchVantage—must be designed to accept passwords and transmit them with proper safeguards.

- Passwords must be prohibited from being displayed when entered.
- Passwords must never be stored in clear, readable format (encryption must always be used).
- Encrypted password hashes must never be accessible to unauthorized individuals.
- Where any of the above items are not supported, appropriate authorizations and access control methods must be implemented to ensure only a limited number of authorized individuals have access to readable passwords.

Password Requirements

The following parameters indicate the minimum requirements for passwords for all individual accounts where passwords are:

- The Password must be between 8-20 characters in length;
- Must not be based on anything somebody else could easily guess or obtain using person related information (e.g., names, CWID, telephone numbers, dates of birth, etc.);
- A combination of at least one character from each of the following four listed character types:
    - English uppercase letters (A-Z),
    - English lowercase letters (a-z)
    - Base 10 digits (0-9)
    - Special character out of !@#$%^&*()\-_=+{};:,<.>

Password Reset Options

Various options are available to assist users with changing a forgotten password. The preferred and fastest method is through the use of the link https://cp.pitchvantage.com/forgot-password/

to safely regenerate your password. You can also contact support to request a change. Your password is encrypted so we cannot access it but we will change your password on your formal request and email your temporary password to you that you can change through your PitchVantage profile.

Reporting a Suspected Compromise or Breach

If you believe your password has been compromised or if you have been asked to provide your password to another individual, including PitchVantage, promptly notify support@pitchvantage.com

Filing or reporting a security incident can be done without fear or concern for retaliation.

Data Transfer

All data transfer between PitchVantage cloud/iOS/Android/Desktop application and servers happen via a secure layer using HTTPS protocol. RESTful web services are used to transfer data between client and server and data transfer happens in JSON standard format

It requires unique encrypted authentication token to transfer user data and thus require user login credential to access user specific data.
It is user's responsibility to protect his/her credentials; we believe user won't share his/her credentials with anyone and maintain his/her data privacy. User's password can be recovered by clicking forgot password on their login page.

Data logs, Monitoring and Recovery

PitchVantage keep activities logs of both Application level and server level.
We keep monitoring those at regular intervals and check for any suspicious incident or unusual activity. If we find anything unusual then we take necessary action to prevent those and if any breach happens, we communicate with anyone who's affected and do everything possible to prevent similar incidents from happening again.
PitchVantage takes automatic data back-up regularly. PitchVantage plans to conduct frequent Penetration testing.

Training, Certification and Compliances

PitchVantage keeps high standards in development and process management. Our team constantly upgrades their knowledge in process, development and security; we provide training to our employees continually to keep abreast with the latest technology, security and compliance standards. PitchVantage follows PCI (Payment Card Industry) compliance. PitchVantage has taken steps to comply with GDPR: https://s3.amazonaws.com/pv-case-studies/PV_GDPR.pdf

FERPA

FERPA is designed to protect student identity and academic information from unauthorized disclosure to third parties. PitchVantage complies with all relevant provisions as follows:

- Students account information is private in the system, viewable only by authorized instructors and PitchVantage administrators. Such permissions must be explicitly granted within PitchVantage.
- No grading information is viable or available within PitchVantage. PitchVantage scores are only relevant within the realm of PitchVantage.
- Authorized PitchVantage team members may access the account information solely for the purpose of providing service and support to the instructor and students. Such access is limited to authorized service and support staff only. Consent for this limited use of their account information is granted by each student user upon signup with required acceptance of the Use Policy and Privacy Policy.

Incident Response Management

Network Protection

PitchVantage's network protections include solutions designed to provide continuity of service, defending against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
We use AWS Firewall and best practices for threat detection.

Monitoring and Event Alerts
Alerts are sent to PitchVantage's cloud security operations teams for review and response to potential threats. These alerts are monitored 24x7x365.

Incident Response
PitchVantage evaluates and responds to events that create suspicion of unauthorized access to or handling of customer data on AWS servers or on the personal hardware assets of PitchVantage employees and contingent workers.
Requirements for incident-response programs and operational teams are defined per incident type:

- Validating that an incident has occurred
- Communicating with relevant parties and notifications
- Preserving evidence
- Documenting an incident itself and related response activities
- Containing an incident
- Eradicating an incident
- Escalating an incident

Upon discovery of an incident, PitchVantage defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is

performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and central systems are utilized to collect information and maintain a chain of custody for evidence during incident investigation.

Notifications
In the event that PitchVantage determines that a security incident has occurred, PitchVantage promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities. Information about malicious attempts or suspected incidents is PitchVantage Confidential and is not externally shared. Incident history is also PitchVantage Confidential and is also not shared externally.

Service Scope and Management

Service Scope:

- Monitored email support
- Telephone support
- Support site and knowledge base (https://support.pitchvantage.com)

Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide relevant details on service availability, monitoring of in-scope services and related components.

Service Availability.

- Availability (Uptime Guarantee): Licensor guarantees 99.9% Uptime each month 24 hours a day 7 days a week (“Agreed Hours of Service”). Uptime is measured based on the monthly average of availability, rounded down to the nearest minute, and calculated as follows:
    - Uptime %= (agreed Hours of Service – hours of downtime)/agreed hours of service * 100
- Monitored email support 7am-10pm Monday-Sunday
- Telephone support is available 8am-6pm Monday-Friday upon user request.
- Requests can be submitted. through email (support@pitchvantage.com) or PitchVantage Support Site (support.pitchvantage.com).
- Support site and knowledge base (https://support.pitchvantage.com) 24 hours a day, 7 days a week.

Service Requests. In the event of a service request, Licensor is deemed to have responded when it has replied to Licensee’s or Licensee User’s initial request. This may be in the form of an email or telephone call, to acknowledge receipt of Licensee’s or Licensee User’s request, provide a solution, or request further information.

The response time and resolution time will depend on the priority of the item(s) affected and the severity of the service request, as set out in the following schedule:

- High priority: Licensed Software is not available for use or a significant portion of the functionalities are not available.
- Medium priority: One or more elements of the Licensed software ceased to respond completely or respond extremely slow.
- Low priority: Notification of minor issue that does not prohibit Licensee or Licensee's Users from utilizing the Licensed software in any material way.

In support of services outlined in this Agreement, the Licensor will respond to service requests submitted by the Licensee and Licensee Users within the following time frames (Resolution Time Schedule):

- 0-2 hours (during business hours, 8am-6pm MST Monday-Friday for issues classified as High priority. Resolution within 5 hours inclusive of response time.
- Within 24 hours for issues classified as Medium and Low priority. Resolution within 24 hours exclusive of the response time.
- Remote assistance will be provided in-line with the above timescales dependent on the priority of the support request.

Problem Management. PitchVantage Support regularly analyses all tickets in order to identify trends and bottle necks. Based on these findings, Support updates the Support Site and Knowledge Base with information explaining the solution to "known errors".

In order to respond to FAQs and help users resolve common problems without needing direct assistance from Support, PitchVantage maintains the Knowledge Base on the PitchVantage website (support.pitchvantage.com).

Mobile Device Policy

Security Mobile Device Management (MDM)

PitchVantage does not allow employee mobile devices to connect to corporate resources.

Confidential Data Policy

PitchVantage requires publicly available data for student registration (university email and name). No confidential data is collected or required from end users. This public data presents a low financial and information risk to the client.
More information on the steps PitchVantage takes to protect user data can be found in the Data Storage and Access Policy section.

IT and Hardware Requirements

Client's IT team needs to ensure **HTTP (port 80)** and **HTTPS (port 443)** access to:
pitchvantage.com
***.pitchvantage.com**

S3.amazonaws.com

Minimum system requirements for both Windows and Mac users:

- Laptop (including Microsoft Surface) manufactured after 2011 with Internal Webcam
- (Recommended) Headset/headphone/earphone with Microphone
- Works with Google Chrome and Firefox web browser

Mobile version (downloadable via iOS App store and Android Play store) minimum requirements

- Minimum system requirement for Apple users: iOS 7+
- Minimum system requirement for Android users: Android 5.0 and above