



HR Avatar

Security Manual

Version 1.26.3 (April 28, 2026)

Are you viewing the latest version?

The latest version is always located at <https://www.hravatar.com/security>

HR Avatar Security Manual

Version 1.26.3

Table of Contents

Transmittal	3
Introduction	4
Control of Document	4
Security Priorities	4
Information Security Organization.....	4
Company President.....	5
Applications Development Manager	5
Information Security Manager (ISM)	5
Incident Response Officer	6
Reporting.....	6
Annual Review	6
Implementation	6
Supporting Documents	7
Latest Version	7
Section 1: Human Resources	8
Practices for New Hires.....	8
Confidentiality / Non-Disclosure.....	8
Practices for Existing Employees.....	8
Practices for Employee Termination.....	8
Practices for Client Account Termination	9
Annual Security Awareness Training.....	9
Cooperation with Client or Partner Auditors.....	9
Physical Security Reviews	10
Security Awareness Control Worksheet	10
Section 2: Employee Responsibilities.....	10
Computer Usage	10
Internet Usage	11

Passwords	12
Information Classifications.....	15
Clean Desk.....	16
Clean Computer	16
Generative AI Use Policy	17
Section 3: HR Avatar Application-Level Accounts and Users	18
Section 4: Information Technology.....	23
Overview of HR Avatar-controlled Systems.....	23
The Authentication Boundary.....	24
Individual Responsibilities.....	24
Cloud-Based Services	24
Information Security Guidelines	25
Credential and Cryptographic Material Management.....	34
Installation of 3 rd Party Software (new 2023)	34
All new 3rd party software to be installed on HR Avatar production systems must be approved by the Application Development Manager and logged in a software installation log. This log shall indicate approval date and installation date, and it shall be reviewed monthly by the Information Security Manager.	34
System Logs and Log Retention	35
Data Backup Policy.....	35
Data Sharing with API Users.....	35
Incident Response.....	36
Housekeeping Log.....	36
Audit and Review	36
Appendix A: Security Incident Log Format.....	38
Appendix B: Incident Response Procedures	39
Appendix C: Employee Termination Checklist	40
Appendix D: Client Account Termination Checklist	41
Appendix E - Prohibited Software and Hardware.....	42
Appendix F: Overview of the Production Infrastructure	43
Appendix G: Summary of Recurring Requirements	44
Appendix H: Version History	45

Transmittal

Date: 28 April, 2026

To: All Employees of HR Avatar, Inc.

From: Michael Russiello, President

Subject: HR Avatar Security Manual – Revision 1.26.2 Issuance

I'm please to present Revision 1.26.3 to our security manual, which I have approved via this cover letter and my signature below.

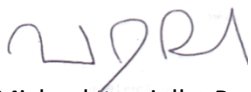
Individual and organizational privacy and safety have always been a core assumption for the customers of any business, regardless of their location on our planet. However, in today's ultra-connected, AI-powered marketplace, businesses and individuals are more vulnerable than ever and can suffer financially and psychologically from a breach of data. Victims include the entities whose data is contained within the breach as well as the organization that allowed the breach to happen in the first place.

In response to these threats, governments are tightening regulations regarding acceptable practices for physical and information security among businesses and organizations that collect personal information about their clients or other stakeholders. Currently, these include the European Union, the State of California, and the US Federal Government.

This document is intended to specify the processes and procedures that we will follow to protect our employees, the company, and our customers. The Security Manual will work in conjunction with our Terms of Use, and or Privacy Policy documents, both of which are maintained on our website at <https://www.hravatar.com/terms> and <https://www.hravatar.com/privacy>, respectively, as well as the security incident log.

A solid security posture is something that is only achieved through a group effort with 100% participation and commitment. I expect everyone on our team to embrace this policy in literal terms as well as in spirit. Our business depends on it. All employees are required to review this manual prior to gaining access to HR Avatar computer systems and data, and annually thereafter. Additionally, managers will conduct periodic reviews of these guidelines to ensure familiarity and vigilance.

Thank you in advance for helping protect our customers' data and helping HR Avatar remain a viable and growing company.



Michael Russiello, President
mike@hravatar.com

Introduction

The purpose of this security manual is to:

1. Ensure the safety of all HR Avatar employees.
2. Safeguard client, employee, and corporate personal and proprietary data.

This document will be updated regularly and incrementally to adapt to the changing security landscape. Please see the revision history contained in the appendix for a summary of recent changes and enhancements.

Control of Document

This document and related documentation can only be updated with approval of the President. A summary of changes made, and approvals must be documented in Appendix H. Each time the document is updated, the approval must be documented in an email to all employees that promulgates the revision.

Security Priorities

Our priorities are, in order of importance:

1. Protect HR Avatar staff for physical or other risk associated with performance of their duties.
2. Protect all client-specific information shared with and stored within HR Avatar systems from compromise.
3. Protect HR Avatar proprietary information from compromise.

Client-specific information refers to all the information created and stored on behalf of a client that is unique to that client. For instance, test-taker or candidate personal data, such as name, email or phone number, user data such as name, email, phone number, and authentication credentials, candidate test result data, such as item responses or score reports and any recorded images, audios, or videos are all considered client-specific information.

HR Avatar is trusted by its clients to safeguard their data against all reasonable threats. Our business depends on our ability to maintain this trust.

Information Security Organization

HR Avatar is a streamlined organization with relatively few employees compared to our competitors. Most staff wear multiple hats and perform various duties. However, in addition to their normal duties, ALL EMPLOYEES play a role in information security. It is critical that all staff take their information security responsibilities seriously and work as a team.

HR Avatar staff are subdivided into three groups:

- Level 1 Staff – Not granted any special rights to client data or production information systems.
- Level 2 Staff - Granted rights to client data and accounts, but not granted administrative rights to production information systems.

- Level 3 Staff - Granted rights to client data and accounts, and administrative rights to production information systems.

There are currently no Level 1 staff. The number of Level 3 staff are minimized to include only the company President, the Applications Development Manager, and the Information Security Manager.

Company President

The company President is responsible for ensuring that the information security organization is staffed and actively engaged in executing its responsibilities. The current President is Mike Russiello at mike@hravatar.com.

Applications Development Manager

The Applications Development Manager (ADM) is responsible for ensuring that the standards in this policy are adhered to in all software development projects.

The ADM is currently Mike Russiello. He can be contacted at mike@hravatar.com.

Information Security Manager (ISM)

The Information Security Manager or ISM is responsible for ensuring that security manual procedures and the intent of these procedures are properly followed.

Important Note: It is often important to maintain separation of supervisory and execution responsibilities so that appropriate checks and balances are in place. In the context of security, this means the Applications Development Manager and Information Security Manager roles should be filled by different people. Unfortunately, in HR Avatar's current organization there is only one person with the required level of knowledge for either of these roles, and a full separation of duties is not possible. As the company grows and additional staff are hired who can fulfill either role, separate individuals will be appointed to the Information Security Manager and Applications Development Manager roles. In the meantime, the Application Development Manager will fulfill the duties of the Information Security Manager. Additionally, in order to provide checks and balances, we have named an Interim Information Security Manager. The duties of the Interim Information Security Manager are:

- A. Track the completion of all administrative requirements contained in the Security Manual, such as reports, training, and reviews.
- B. Provide an annual report to the President regarding discrepancies between what has been accomplished versus the requirements of the manual. The annual report shall be stored in shared storage so that it can be retrieved during any subsequent security audits.

The Interim Information Security Manager is Sandy Stiltz. Ms. Stiltz can be contacted at sandy@hravatar.com or +1-703-688-3981.

Note: The Applications Development Manager currently also functions as the HR Avatar Privacy Administrator.

Incident Response Officer

The Information Response Officer is responsible for taking charge of all immediate response actions in the event of a security incident.

The Incident Response Officer is currently Mike Russiello. He can be contacted at mike@hravatar.com or +1-703-688-3981.

Reporting

The Information Security Manager will prepare annual and monthly reports covering security-related initiatives and policies, and addressing any known issues or incidents that have occurred during the reporting period.

Annual Report (revised 2023)

This report shall be delivered to the President. Previous reports shall be retained for at least 2 years for audit purposes.

The Annual Report shall serve as a formal review of the company's security program and shall observations, discussion, and recommendations. The Annual Report is a forward-looking document that contains actionable suggestions.

Monthly Reports (revised 12/2023)

There are no formal monthly reports. However, the Information Security Manager should review the following with the President on a monthly basis:

- Program activities
- Incidents and Remedial Actions
- Software Updates and Patching
- Employee Terminations
- Vulnerability scanning results.

The purpose of these monthly discussions is to ensure that adequate attention is being placed on information security throughout the year.

Annual Review

This manual and its underlying policies are continually evolving as new practices are incorporated. However, at a minimum, the manual will be reviewed at least annually by the Information Security Manager for compliance with the latest laws and regulations, as to ensure that HR Avatar's practices remain up-to-date.

Date of Last Review: 4/15/2026

Implementation

Unless noted below the practices denoted below are to be implemented immediately. Any item of non-compliance that cannot be quickly rectified should be reported to the Information Security Manager.

Supporting Documents

The HR Avatar Terms and Conditions (<https://www.hravatar.com/terms>) outlines terms and conditions applicable to users of any HR Avatar website. While not specifically connected with security, the Terms and Conditions do specify an implicit agreement between client and HR Avatar. The company's security practices constitute a key pillar in executing the HR Avatar side of this agreement.

Additionally, the HR Avatar Privacy Policy (<https://www.hravatar.com/privacy>) specifies HR Avatar's commitments to users of its services regarding protection of individual and customer data. Similar to the Terms and Conditions, the company's security practices are an integral component of the method used to live up to commitments in the Privacy Policy.

The following additional documents also play a role in the administration of our security program:

- *HR Avatar Security Incident Response Log and Procedures (See Appendices A and B)*
- *HR Avatar Software Development Procedures ***
- *HR Avatar Risk Assessment Process ***
- *HR Avatar Business Continuity Plan ***
- *HR Avatar Production Network Diagram ***
- *HR Avatar Standard Service-Level Agreement (<https://www.hravatar.com/sla>)*
- *HR Avatar Organizational Chart ***
- *Employee Security Manual Review Acknowledgement Form (<https://www.hravatar.com/secman-acknowledge>)*
- *Employee Non-Disclosure Agreement (<https://www.hravatar.com/nda>)*
- *Client Data Processing Agreement (<https://www.hravatar.com/datasharing-client>)*
- *Partner Data Processing Agreement (<https://www.hravatar.com/datasharing-partner>)*
- *Partner Security Questionnaire (under development)*

*** Access removed and document marked as Confidential and treated as a controlled document (4/2023)*

Latest Version

The most up-to-date version of this document is always located at <https://www.hravatar.com/security>.

Section 1: Human Resources

The weakest security link in an organization is staff ignorance. HR Avatar recognizes that we are no exception.

Practices for New Hires

HR Avatar handles personally identifying information (PII) for many individuals. Therefore, new hires should be carefully screened to ensure they have no criminal intentions or tendencies.

Background Investigations

Starting 1 August, 2018, new full-time employees must have a background investigation that looks back at least 7 years for criminal activity, verifies educational credentials, and checks the national sex offender database.

New part-time or freelance hires, or independent contractors do not require background investigations unless a specific contract requires them, or unless the nature of their work will expose them to customer or employee personal information.

In-Person Interview Requirement

Due to the emergence of deep fake job candidates, every full-time candidate for HR Avatar will be interviewed in-person prior to hiring and receiving access.

Confidentiality / Non-Disclosure

Starting 1 September 2018, all employees (new and old), as well as contractors who have direct access to company assets or data, must sign the company's employee confidentiality and non-disclosure agreement, or a mutually acceptable business-to-business non-disclosure agreement. In addition to protecting company assets, this is a mandatory element for protecting client data.

Security Indoctrination

Before being granted access to any HR Avatar data or security systems, new hires (both full time and part time) will be required to read these security guidelines and acknowledge their understanding by signing the Employee Non-Disclosure Agreement (<https://www.hravatar.com/nda>) and Employee Acknowledgement (<https://www.hravatar.com/secman-acknowledge>).

Practices for Existing Employees

Employees who are already employed at the time of transmittal of this policy must review the policy and discuss it with their manager, and then they must complete and sign the Annual Security Manual Review - Employee Acknowledgement form.

Following the initial acknowledgement, all employees should review and discuss the procedures included in this manual annually. Additionally, a meeting should be held where managers will review the Security Incident Log with staff to ensure past mistakes are not repeated.

Practices for Employee Termination

An employee termination checklist (see the Appendix) shall be completed and presented to the Information Security Manager following each employee termination.

All passwords for departing employees, Levels 1, 2 and 3, shall be disabled within 1 hour for employees terminated for cause, and 24 hours for employees leaving for reasons other than cause. Any generic system passwords will be changed within these timeframes as well, if applicable.

Employee business applications (such as email and cloud-based storage) will be terminated or transferred within 24 hours and all data archived, unless the President determines that an extension of certain applications (such as email) is appropriate and justified. Typically, departed employee data are temporarily transferred to another employee to allow for continuity in serving clients and partners during the transition period of no more than 6 months after an employee departs. Following this period, all data should be deleted.

AWS IAM users and privileges will be reviewed. If the employee had access to any IAM users with password access the password must be changed. If the employee had access to any API keys, the API keys must be refreshed.

Practices for Client Account Termination

Many larger client accounts have contractual requirements for account termination, including removal/pseudonymization of data from all information systems, and removal/deactivation of client user logons to applications. These contractual requirements always take precedence over HR Avatar procedures.

The Client Account Termination Checklist is provided in the Appendix.

Annual Security Awareness Training

The Information Security Manager will conduct annual security awareness training for all employees on at least an annual basis. Performance of training shall be documented in a security awareness control worksheet.

Security bulletins shall be issued when appropriate and documented in the security awareness control worksheet. At least annually a security bulletin that emphasizes specific requirements from this manual should be transmitted to employees, preferably at the midpoint between training sessions.

During the annual refresher training the Risk Assessment Process will be covered and the current Risk Identification Worksheet reviewed by all employees.

The annual refresher training will include a review of the Security Manual by each employee. Each year, every employee must sign an acknowledgement (<https://www.hravatar.com/secman-acknowledge>) that they have reviewed the Security Manual and are willing to fully comply with all requirements included within it.

Date of last training: 4/18/2026

Cooperation with Client or Partner Auditors

When cooperation and information sharing is requested by a client or partner for the purpose of validating HR Avatar information security practices and procedures, the Information Security Manager

will coordinate all activities and will cooperate to the maximum degree practical without compromising HR Avatar's security posture.

Physical Security Reviews

If HR Avatar obtains any physical facilities (currently the company is completely virtual), HR staff or the Information Security Manager may conduct impromptu audits of physical facilities and equipment to ensure compliance with HR Avatar security procedures. Violations will be pointed out to employees for correction. Repeated or serious violations will be reported to the Information Security Manager.

Security Awareness Control Worksheet

A Security Awareness Control Worksheet will be maintained by the Information Security Manager to document security awareness activities such as new employee indoctrination, training, and bulletins.

Section 2: Employee Responsibilities

Computer Usage

HR Avatar provides employees with access to computers, computer files, email, and software. The company may monitor usage of all of these assets to ensure that this policy is followed.

Employees are not allowed to use computers and email in ways that are disruptive, offensive to others, or harmful to morale.

Employees should:

- Never interfere with or disable virus protection software on computer equipment unless necessary for software development / maintenance activities.
- At minimum, perform anti-malware and virus scans on a monthly basis or more frequently if warranted. A tool such as Windows Defender or Malware Bytes Anti-Malware should be used.
- Configure computers so that downloaded files are always placed in the same directory and that this directory is periodically cleaned either by an automated tool such as CC Cleaner, or manually by a qualified information technology professional.
- Ensure that access to desktop computers and mobile devices is password or biometrically protected.
- Not display, download, or email sexually explicit images, messages, and cartoons, and not use computers and email for ethnic slurs, racial comments, off-color jokes, or anything that another person might take as harassment or disrespect.
- Not use email to ask other people to contribute to or to tell them about businesses outside of HR Avatar religious or political causes, outside organizations, or any other non-business matters.
- Not use software licensed for one computer on more than one computer.
- Only use software on local area networks or on multiple machines according to the software license agreement.
- Not illegally duplicate software and its documentation.

Any employee who knows about any violations to this policy should notify management immediately. Employees who violate this policy are subject to disciplinary action, up to and including termination of employment.

Internet Usage

All Internet data that is written, sent, or received through HR Avatar computer systems or using an HR Avatar email address is part of official HR Avatar records. The company recognizes that it can be legally required to show that information to law enforcement or other parties.

ALL EMPLOYEES ACKNOWLEDGE that their company email history and data is part of HR Avatar official records.

HR Avatar reserves the right to monitor how employees use the Internet, and to find and read any data that employees may write, send, or receive through online connections.

Employees may not write, send, read, or receive data through the Internet that contains content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person.

Examples of unacceptable content include (but are not limited to) sexual comments or images, racial slurs, gender-specific comments, or other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

HR Avatar does not allow the unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet.

Employees who use the Internet in a way that violates the law or HR Avatar policies will be subject to disciplinary action, up to and including termination of employment, and may also be held personally liable for the violation.

The following are examples of prohibited activities:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using the organization's time and resources for personal gain
- Stealing, using, or disclosing someone else's code or password without authorization
- Copying, pirating, or downloading software and electronic files without permission
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization
- Violating copyright law
- Failing to observe commercial licensing agreements
- Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions

- Sending or posting messages or material that could damage the organization's image or reputation
- Participating in the viewing or exchange of pornography or obscene materials
- Sending or posting messages that defame or slander other individuals
- Attempting to break into the computer system of another organization or person
- Refusing to cooperate with a security investigation
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Using the Internet for political causes or activities, religious activities, or any sort of gambling
- Jeopardizing the security of the organization's electronic communications systems
- Sending or posting messages that disparage another organization's products or services
- Passing off personal views as representing those of the organization
- Sending anonymous email messages
- Engaging in any other illegal activities

Passwords

Virtually all systems and data can be accessed through passwords – though remote access to HR Servers do not allow password logins. Therefore, a key component of our security posture is password protection.

Passwords must comply with, and be enforced by applications where applicable, with the relevant password policy described below.

If an incident occurs in which one or more passwords may have been compromised, the Information Security Manager should be notified and relevant passwords changed immediately.

Users with System-Level and Database Access

HR Avatar Production servers do not allow password-based authentication for remote administrative access. Instead, they rely on use key-based authentication only for remote access. Additionally, remote root login is not permitted.

However, important applications such as web-servers, databases, and administrative web applications do require password authentication in some cases. Passwords that grant production system-level access (e.g., root, enable, admin, application administration accounts, etc.) for systems that process or store client data should be changed every 365 days. Passwords granting administrative access to either operating systems or administrative access to critical production applications shall be at least 12 characters in length and must comply with other standard password construction rules (described below). This standard includes accounts with system-level privileges granted through group membership.

General Users

All user passwords (e.g., email, web, desktop computer, etc.) for HR Avatar web applications should be changed every 365 days. Passwords must not be included in email messages or other forms of electronic

communication. Additionally, when changing a password, the previous 4 passwords must not be re-used.

HR Avatar production applications are configured to accept only strong passwords (per rules below) when users register or change their passwords. All users are required to change their passwords once per year. Users with administrative access – access to other accounts – are required to have passwords that are 12 characters in length. Other users, with access only within their accounts, are required to have passwords that are at least 12 characters in length and no more than 64 characters in length.

Password Construction Guidelines

General password construction guidelines are used for various purposes at (organization), i.e. user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins). It is important that everyone be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password can be found in a dictionary (English or foreign)
- The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, computer terms and names, commands, sites, companies, hardware, software, birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc. Any of the above spelled backwards. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@\$%^&*()_+|~- =\`{}[]:~>?<./)
- Are at least eight alphanumeric characters in length and no longer than 64 characters.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Do not have repeating sequences of characters or numbers of length 3 or more.
- Do not have sequential numbers or letters of more than 3 or more.

HR Avatar web applications incorporate automated tools that require passwords to comply with the above guidelines.

The current password rules are as follows:

Between 12 and 64 characters long (15 or higher for system admins)

Must contain at least 3 of the following:

- (a) One or more lowercase letters,
- (b) One or more uppercase letters,
- (c) One or more numbers, or

(d) One or more special characters (~\!@\$%^&*()_~).

Characters that are not allowed include single quotes ('), double quotes ("), hash (\#), and double dashes (--).

Cannot use common words or phrases.

Cannot have repeating sequences of characters or numbers of 3 characters or more.

Cannot have sequential sequences of characters or numbers of 3 characters or more.

Finally, passwords are always case sensitive.

Password Protection

All passwords stored electronically should be stored in the database in an encrypted format only.

Employees should:

- Change passwords at least once every 365 days.
- Not write down passwords.
- Passwords should never be stored in a freely accessible document or file, either in hard copy or on a computer. Passwords should only be written down within an encrypted “vault” protection program designed to protect them. Examples of acceptable vault programs are KeyPass (<https://keepass.info/>) and Password Manager Pro (<https://www.manageengine.com/products/passwordmanagerpro>)
- Not store passwords on-line without encryption.
- Not use the same password for (organization) accounts as for other non-(organization) access (e.g., personal ISP account, on-line banking, email, benefits, etc.).
- Not share (organization) passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential (organization) information.
- Not reveal a password over the phone to ANYONE
- Not reveal a password in an email message
- Not reveal a password to the boss
- Not talk about a password in front of others
- Not hint at the format of a password (e.g., "my family name")
- Not reveal a password on questionnaires or security forms
- Not share a password with family members
- Not reveal a password to co-workers while on vacation
- Not use the "Remember Password" feature of applications.
- If someone demands a password, refer them to this document or have them call the IT Manager.
- Report any incident in which a password may have been compromised to the IT Manager immediately.

Failed Logon Policy

HR Avatar applications are configured so that if there are five failed consecutive logon attempts to a specific username, the user is “locked out” for 30 minutes. During this enforced wait period, only a user with system admin privileges can unlock the user.

Unusual Logon Policy

When a user signs in from a different IP address than used in the past, and the new IP address is associated with a different country than their previous logons, the system will send them an email notifying them of this logon, in case it is a breach. Users can opt out of these messages if they want.

Other Password Guidelines

Passwords assigned by software publishers or factories are to be changed immediately upon installation on production systems.

Passwords or Key Pairs for group/role accounts on production servers should be changed when membership in the group by individual users is changed (ie someone with access leaves the company).

Password Resets

Password resets should be conducted by customer service representatives after authenticating the user using at least two independent pieces of information or by an automated password reset link that has a 1-hour expiration and that uses encrypted information so that username and password cannot be extracted from the link.

Multi-Factor Authentication

HR Avatar now supports optional multi-factor authentication (MFA). Individual accounts can require that all account users use MFA in order to gain access to account information.

While MFA is optional for account-level users, all system-level user accounts (Overall System Administrators) must use MFA.

Information Classifications

HR Avatar uses the following Information Classifications when addressing client data:

Classification	Description
Confidential	Personally identifying information (PII). Other data deemed proprietary to specific clients such as test results traceable to a specific individual, photos, videos, audios of test candidates, demographic information regarding candidates. Registered user logon information and logon history/activity.
Public	Unprotected data.

The vast majority of information managed by HR Avatar, including ALL CLIENT DATA is CONFIDENTIAL.

Clean Desk

An effective clean desk effort helps protect paper documents that contain sensitive information about our clients, customers and vendors.

Employees should:

- Place sensitive working papers in locked drawers during known extended periods away from their desk, such as a lunch break, or a scheduled meeting.
- Before leaving for the day or for an extended period, ensure that their desk is tidy and all sensitive working papers are stored in locking desks and file cabinets and that any desktop computing devices are turned off or placed in password-protected sleep mode.
- Treat portable computing devices and mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
- Where practical, avoid the use of paper documents entirely by scanning and storing documents electronically in password-protected locations.
- Avoid creating documents that contain any client personally identifying data, such as reports with email addresses.

In the Office

Within any office environment maintained by HR Avatar (there currently are none), HR or executive staff may conduct impromptu audits of physical facilities and equipment, including employee desks, to ensure compliance with HR Avatar security procedures. Violations will be pointed out to employees for correction. Repeated or serious violations will be reported to the Information Security Manager.

At Home

HR Avatar staff working from their homes must also take steps to ensure that HR Avatar information is protected. Employees must be careful to protect HR Avatar computer assets as well as physical papers when storing them in their home. These items should be stored in a hidden location when not in use and paper files containing client data should never be stored in home locations for more than a few days.

Clean Computer

HR Avatar staff frequently access client data, either to help with score interpretation, train account users, perform test development and maintenance activities, perform fairness and or validity studies, or to prepare custom one-time reports. Therefore, it is important for staff to keep a clean “computer” in addition to a clean desk.

All files downloaded from HR Avatar applications, such as CSV files and PDF files should be placed in the same folder, typically called “downloads.” This folder should be periodically cleaned out using a tool such as CC Cleaner.

Employees should organize their computer's file structure thoughtfully, so that data is easily located. Data that is no longer needed should be deleted.

HR Avatar executives have the right to confiscate an employee's computer and review the file structure and files contained to verify compliance with this guideline of a clean computer. Serious or repeated violations should be reported to the Information Security Manager.

The computer should enter a password-protected standby mode after a period of inactivity, no longer than 30 minutes.

When a user will be away from their desk for any amount of time, any applications with administrative access to production systems, such as a database query tool or file manager, should be closed.

Generative AI Use Policy

Artificial Intelligent (AI) can vastly improve productivity and creativity and, ultimately, impact the way companies like HR Avatar deliver value to customers. At the same time, AI can be harmful to customers and potentially to HR Avatar due to compromised privacy, non-compliance with various laws, and other types of misuse.

It is therefore critical that employees:

- Become familiar with AI and its capabilities
- Apply AI tools safely and responsibly.

To increase familiarity, employees are encouraged to read, discuss AI usages, and experiment with approved tools to streamline workflows.

To ensure responsible application of AI tools throughout the business, employees must comply with the following guidelines:

1. Use mainstream free public AI tools like Google Gemini, OpenAI, Meta, and Claude for general search and information gathering purposes only.
2. Never input confidential, proprietary, or client-sensitive data into public AI tools. This includes names and other personally identifying information.
3. Never upload proprietary information to public AI Tools.
4. Use only approved AI tools when working with proprietary data.
5. Employees are always responsible for the accuracy of AI-generated output. When using AI tools, employees must always fact-check and edit results before sharing them internally or externally.
6. Clearly disclose when a significant portion of a deliverable was created using AI.
7. Never use AI to create harmful, discriminatory, or deceptive content, or to impersonate others for fraudulent purposes.
8. When designing AI-based tools into HR Avatar's products or services, AI-derived scores and inferences should always be annotated to ensure that customers know the source of the data was AI.

9. Ensure the appropriate disclosures are made to all stakeholders – clients, candidates, and employees when AI is used to process their information.

Section 3: HR Avatar Application-Level Accounts and Users

Application-Level Accounts

All HR Avatar products are accessed via application-level accounts. Application-level accounts are created by individuals who register for an HR Avatar account on behalf of their company by filling out a web form. Once an account is established, additional users can be added, modified, or deleted as described below.

Application-level accounts require email-based validation prior to activation.

Automated processes are run periodically that can disable and close application-level accounts, based on lack of user activity. Accounts are placed in “Disabled” status after 2 years of inactivity. When in “Disabled” status, accounts cannot be accessed by clients and no testing can occur. However, HR Avatar staff can access the account and can re-activate if appropriate. Additionally, accounts are “Closed” after 5 years of inactivity. Once closed, all user data is automatically pseudonymized and these accounts can no longer be accessed or reactivated.

Application-Level Users

A user record within the HR Avatar system refers to an entity that has personally identifying information associated with it. User records are utilized for HR Avatar staff and clients who create assessments, view results, and perform miscellaneous other activities in support of the business. User records also include candidates themselves, who complete tests typically at the request of a client.

Every user on the HR Avatar system has a role definition. The active role definitions are included in the table below:

User Role	Description
No logon	Users who cannot log on to the system. Typically, these are candidates who have been asked to complete an assessment, reference check, or video interview by a client.
Personal	Same as No Logon role. Currently not in use.
Portal	Users who are granted access for repeated use of a testing portal. This can be for users who want to complete practice assessments from time to time. This feature is currently not in use.
Can Create and View Incomplete Test Keys Only	Can send assessments, recorded video interviews, and live video interviews. Can review incomplete tests and incomplete video interviews/invitations. Cannot view results.

Can View All (Read-Only)	Can view incomplete assessments and test results. Can view reference checks. Can view incomplete and completed recorded video interviews. Can view live video interview invitations and results. Cannot send or edit assessments, reference checks, and video interviews (live and recorded).
Can View Incomplete Tests Only	Can review incomplete tests, the test catalog, and incomplete video interviews/invitations. Cannot view results.
Basic User	Can create tests in the Custom Test Builder, edit/create reference checks and video interview scripts. Can administer assessments to candidates, view incomplete tests, view test results, and bulk download results in a spreadsheet or PDF. Can create and send test batteries. Can create reference check templates, send reference checks, and view reference check results. Can create live and recorded video interview scripts, send invitations, and view results of live and recorded video interviews. Can view other users in the account but cannot add/delete users or adjust account settings.
Basic User with no Spreadsheet or PDF bulk download	Same as basic users but cannot download results in bulk, either in spreadsheet or zip file format.
Account Administrator	Same as basic users but can also control account settings and other account users.
Overall System Administrator	Reserved for authorized HR Avatar staff only (Security Level 2 or higher). Allows complete access to all client accounts. Requires passwords of 15 characters or higher.

User Type

All users belong to one of three User Types:

1. **Named** – for HR Avatar staff, client administrators, and candidates that have personally identifying information provided by a client or the user.
2. **User ID** – for candidate user records that use a client-assigned assigned identifier. Typically, clients retain a key associating User IDs with actual people. To start an assessment the candidate must enter the User ID that was assigned to them.
3. **Username** – for candidate user records where the user is assigned an arbitrary username and a password by the client. Typically, username and passwords are issued separately to the candidate. To start an assessment the candidate must enter both their username and password.
4. **Anonymous** – for user records that contain no PII.

5. **Pseudonymized** – for account that were named but have had all PII removed through a pseudonymization process.

Additionally, account users can be granted whole organization or sub-organization-only access.

Users are forced to comply with HR Avatar password guidelines. Accounts may also optionally require multi-factor authentication for all users that have access to their account.

All HR Avatar applications are configured to prevent access to application functionality until expired passwords have been reset.

User Anonymity

Most HR Avatar users are candidates who have been asked to complete an assessment, reference check, or video interview by a client. These candidates typically have a User Role of “No Logon.” Initially, candidates are assigned a User Type of “Named,” “User ID,” “Username” or “Anonymous.” These users are pseudonymized at a later time in accordance with the client account’s pseudonymization policy. The users and all test result data are ultimately deleted in accordance with the client account’s data retention policy.

As described above, there are five levels of user anonymity which defines the information used to uniquely identify the candidate user. The levels of User Anonymity Type are:

1. Named: First Name, Last Name, Email
2. User ID: Client-assigned Unique Id
3. Username: Client-assigned Username / Password
4. Anonymous: Randomly generated identifier
5. Pseudonymized: All identifying information obfuscated (pseudonymized)

For situations in which the client does not wish for HR Avatar to store name and email for a candidate, the client can opt to use one of the three other non-pseudonymized methods. User Anonymity Type applies only to candidates and can be set at the account, sub-organization, or specific candidate level.

Proctor File Purging

For both cost-savings and privacy reasons, images, videos, and audios captured during remote test proctoring are deleted after 15 months. This is more than enough time for validation of the authenticity of a candidate or employee.

Pseudonymization

PII should not be stored on HR Avatar systems any longer than necessary to support the needs of the client’s business. However, most PII is associated with individual test responses, and response data is important to testing companies like HR Avatar. Response data is used to calibrate assessment scoring parameters, generate score percentiles, and analyze test fairness across sub-groups of individuals. Therefore, rather than deleting all data for an individual, the data is “pseudonymized.” Pseudonymized means that all PII associated with a given test record is converted to randomized alphanumeric strings,

while high-level demographic info like age and ethnic group, as well as response and score data are preserved.

During pseudonymization, all photos, images, and audios of the candidate are also deleted completely from HR Avatar systems and backup systems.

Clients can set the desired periodicity for automatic pseudonymization of their test taker users. The default value is 2 years, which means that if a user has had no activity within a client account for 2 years, the user is automatically pseudonymized.

Any user (test-taker or client) may request immediate removal of their data from HR Avatar systems. HR Avatar system administrators can use the online applications to quickly accomplish this by pseudonymizing the user's account.

Notes regarding pseudonymization:

- When a user is pseudonymized, all uploaded media files including images, audios, and videos are automatically deleted permanently. Additionally, all personally identifying and cross-reference-able information is converted to randomized alphanumeric strings. This makes the user permanently anonymous.
- Users whose IP address indicates they are from the European Union are automatically assigned a maximum pseudonymization periodicity of 2 years. This cannot be overridden by account-level settings.
- This feature was introduced in July 2018 and all existing accounts were automatically placed on a pseudonymization period of 5 years. All new accounts are currently placed on a 36-month pseudonymization periodicity. Any account administrator can change this value via their online settings.
- Users with account logons are never pseudonymized unless the account is placed into a "closed" status. Accounts can be placed into "closed" status by HR Avatar administrators, or automatically if there has been no activity of any kind for five years.

Automatic Account Disablement

As further protection for client accounts, any client account that has had no activity in the past 2 years is automatically placed into "disabled" status. Users attached to accounts that are in disabled status cannot log on until the account is re-activated by an HR Avatar administrator.

Reviewing automated degradations in account status.

After 2 years of inactivity – Account is disabled. Requires HR Avatar administrator to re-activate.

After 5 years of inactivity – Account is closed. Once closed, all information, including account users (administrators who can log on to administer an account and view test results), is pseudonymized.

Automated User Disablement

In addition to entire accounts, individual account users (users with client account logon access) are disabled automatically when the following certain conditions are met:

- No activity recorded for 24 months or the account pseudonymization period whichever is longer.

Note that account users are not pseudonymized unless the account has been 'closed.' This is why automated user disablement is required for inactive users who have account access.

User account disablement prevents a user from being able to sign in to an account. The password reset capability is also disabled, forcing the user to contact HR Avatar to be reinstated.

Automatic Data Removal Policy (Data Retention Policy)

Though not directly related to security or privacy, HR Avatar also enforces a data retention policy. All customer accounts are assigned a Data Retention Period. The default data retention period is 3 years for accounts created after July 11, 2019 and 4 years for accounts created before July 11, 2019. Data retention periods can be adjusted from 1 year thru 99 years based on customer requirements. Customers can request changes to their data retention period.

When test results or other 'perishable' data entities, such as test keys, expired credit records, and customer service requests become older than the assigned data retention period, these records are deleted permanently. When test results are deleted, all database records containing results information are deleted. These include any image files, video files, or audio files that were collected during the test, and all item responses. Any user records that are also connected but not connected to entities that are less old than the data retention period and also deleted.

The Data Retention Period and Data Pseudonymization Periods and their processes are completely independent of one another. Data pseudonymization is intended to limit damage in the case of security breaches. Data retention is intended to prevent the database from bogging down and to prevent unnecessary data storage costs.

Section 4: Information Technology

HR Avatar systems store personally identifying information (PII) about client employees and applicants. Further, due to the nature of HR Avatar's business, this information is shared through authorized access to HR Avatar web interfaces, as well as through email and SMS telecommunication systems.

Therefore, it is important that the entire production configuration be set up so that unauthorized access to this information is prevented.

Overview of HR Avatar-controlled Systems

The following overview defines the scope and boundary of the systems covered by this policy.

Our systems can be divided into four categories:

1. Production Services - Amazon AWS Platform
2. Production Services - Other Cloud Services
3. Business Applications – Cloud Services
4. Local Computers, Devices and Networks

Amazon AWS: The HR Avatar production systems are located within the Amazon AWS "Cloud." AWS operates as a virtual data center that provides all functions needed to support our business from an information technology standpoint. This includes:

- Computers and Servers (web servers for all HR Avatar applications)
- Databases (to store data)
- Disk Drives (to store files)
- Telecommunications and Network Control Systems
- Various point applications to perform specific tasks, like load balancing, firewalls, text translation, text-to-speech, facial recognition, natural language processing, etc.
- Various services that assist in information security.

Other Production Cloud Services: The AWS systems also access cloud services located outside of Amazon AWS. These include

- Twilio (sms services)
- Dialpad – VOIP Services
- Big Tin Can (Formerly Voice Vibes) (voice analysis)
- CopyScape (plagiarism detection)
- IpStack (IP-based geolocation)
- GoDaddy for some SSL certificates.
- CareerOneStop for job-related information and statistics.
- Hubspot – for Customer Relationship Management.
- Intruder.io – network vulnerability scanning

- Sentino.io – For text analysis services.

HR Avatar applications typically access these applications using API keys or other secure authentication techniques.

Business Applications: Next, we provide various business services to our staff to enable them to perform their job. This includes telecommunication services (phone service), email, virtual storage, web conferencing, and shared documents. These are provided by Google Workspace and DialPad (for phone).

Local Computers and Devices: Finally, all HR Avatar staff have their own computer assets which they utilize when working remotely.

Together these four component categories make up the HR Avatar information systems ecosystem.

The Authentication Boundary

When we discuss authentication and access in general, we are addressing all four categories.

Individual Responsibilities

This means that individuals are responsible for managing their own computer assets and devices in accordance with these guidelines. You are responsible for your own computers and devices. If appropriately authorized, you may also be responsible for cloud-based systems that are part of our ecosystem.

Cloud-Based Services

HR Avatar does not maintain any computer or telecommunications hardware for its production infrastructure. Rather, the entire implementation is hosted by cloud-based services.

HR Avatar uses mainstream cloud-based services for both general business applications (email, calendar, shared storage, documents, etc.), and proprietary applications associated with the service it provides to clients.

These services offer a trusted infrastructure, utilized by literally millions of organizations, that offers reliability, enhanced privacy, and independently-audited compliance with internal procedures, professional standards, and government rules and regulations. They also offer centralized administration that enables consistent application, monitoring, and enforcement of security-oriented policies across applications and across the plethora of mobile and desktop devices now in use.

Various proof of compliance instruments are available from our cloud-based business application providers, such as a SOC3 report (independent audit of compliance with security controls), and an ISO 27001 certificate.

Amazon AWS also maintains a series of third-party audit reports, including SOC1, SOC2, and SOC3. These are further described here:

<https://aws.amazon.com/compliance/soc-faqs/>

Cloud Services in Use - General Business Applications

HR Avatar uses the Google Workspace Suite for its primary business applications (email, calendar, web-conferencing, shared storage, documents, etc). The company also uses cloud-based telecommunication services for telecommunications (telephones and teleconferencing) via DialPad.

Cloud Services in Use – Operations Applications

HR Avatar uses Amazon Web Services (AWS) as its primary production delivery platform. AWS offers numerous features for data protection and access control. Additionally, services Twilio Telecommunications cloud are utilized for SMS messaging, services from Big Tin Can (formerly Voice Vibes) are used to analyze audio files, services from Sentino.io are used for semantic text analysis, and services from CareerOneStop are used to obtain job-related statistics. Plagiarism detection services are provided by CopyScape, IP geo-location services are provided by IP Stack. DNS services are provided by Amazon AWS (Route 53). Private/Public key-based certificate services are provided by Amazon AWS and GoDaddy. Finally, Intruder.io is used to perform automated penetration testing.

Information Security Guidelines

General Business Applications

Cloud-based services associated with general business applications (such as Google Workspace) are mostly managed by the cloud-based service provider. Services are typically managed on a user-account basis. Accounts are created by the system administrator when needed by an employee or an application. Accounts are either transferred or terminated within 24 hours of employee termination.

Where possible and necessary (password authentication is generally avoided), password and other authentication parameters are set to meet standards mentioned in this manual.

Cloud Services Access from Users and Applications

Individual users requiring access to cloud services are granted access via specific IAM User accounts created on Amazon AWS or the cloud service to be accessed. Permissions for these user accounts are limited to what the user needs access for only. When a user leaves the company this user account is inactivated.

IAM User Accounts will be reviewed on a monthly basis to ensure that unnecessary accounts are removed/deleted.

Applications requiring access to cloud services also use IAM User accounts created specifically for them or the group of services they require. These user accounts are authorized for API access only and cannot be used by others to log on to the service console.

Where possible, root access for cloud services (such as with Amazon AWS, and GoDaddy) will have multi-factor authentication activated.

Only the President and the Information Security Manager will have rights to create new Amazon AWS IAM user accounts via the Administrator IAM Role. All accounts will be created via the interactive

interface. The Amazon AWS Console for IAM will be used for creation and maintenance of all IAM accounts.

For administrative access, different IAM accounts will be controlled for both API and console-level access, and user rights will be restricted to allot the least privilege to users necessary to perform their tasks.

Cloud Services Access from API Keys

Certain cloud-based services are accessed via API keys or key pairs. In cases where these keys are utilized and the keys provide access to protected information or assets, the API keys should be rotated whenever it is suspected that there has been a compromise or after an employee with access to a specific key has been terminated.

Administrative Rights

User accounts with system administrative access rights will be controlled by the Information Security Manager. As a rule, a maximum of two users will retain system administrative rights that enable root access to core AWS services.

Application user accounts should minimize the number of accounts having application-level administrative privileges.

Use of Available Cloud-Platform Security Services

The following Amazon AWS cloud-based security enhancement features are currently utilized:

Amazon IAM – to manage user accounts and restrict access to need-to-know, segregate API vs interactive access, and apply least privilege principles.

Amazon Trusted Advisor – to check overall infrastructure configuration and identify weaknesses.

Amazon Inspector – to evaluate all individual resources such as ec2 instances and identify vulnerabilities.

Amazon Shield (part of WAF) – to protect against denial-of-service (DOS) attacks.

Amazon Web Application Firewall – to protect against cross-site scripting, sql injection, and bad bots.

Amazon Guard Duty -- A system that monitors infrastructure activity and applies machine learning to identify intrusions or emerging threats.

Amazon Certificate Manager – to manage SSL certificates.

Amazon Key Management Service (KMS) – to manage cryptographic keys.

Amazon Systems Manager – for hot patching.

Amazon Backup – to perform automated backup of critical resources at fixed intervals

Intruder.io – Periodic (annual) network vulnerability scanning.

BlackKite – Automated vulnerability scanning.

Guidelines for Operations Applications

The following exhaustive list of guidelines should be reviewed by IT staff each year. The Information Security Manager should also review the guidelines with IT staff as needed to ensure compliance.

General

- No client financial data (such as credit card information) shall pass through HR Avatar systems for any purpose. To manage electronic payments without touching client financial data, services such as Braintree Payments will be utilized, which manage financial data directly between the customer and Braintree without using HR Avatar as a go-between, and without exposing any such information to HR Avatar.
- Additional security capabilities made available by the payment processor, such as 3D Secure verification shall be incorporated into e-commerce systems to minimize HR Avatar liability for fraud.
- Remote access to assets containing client data is always via secure encrypted connection (such as HTTPS [TLS 1.2 or higher], SCP, or SSH). This includes any remote database access.
- Public access to any S3 bucket (files) must be accompanied by an S3 policy that requires HTTPS.
- Connections to third-party REST-based Web Services which transfer any data related to clients must be accomplished through HTTPS using TLS 1.2 or higher.
- Connections (web services) to the HR Avatar assessment integration API must be conducted using HTTPS.
- SSH or SCP access to assets containing client data should utilize a public/private key pairs for authentication rather than password authentication.
- All production servers allow remote login only via secure exchange of public/private key pairs and do not allow for password authentication.
- Direct remote root login to production servers is not permitted.
- Passwords used for remote database access and remote application administration must be at least 12 characters in length, and be changed every 365 days.
- No credit card or other financial data (other than amounts charged) should be stored anywhere within the production platform (database or log files).
- Client data (other than credit card or financial data) may be permanently stored only within the database (Amazon RDS) and in secure, encrypted cloud-based file storage (Amazon S3) for binary media files. Any media asset containing client data shall be encrypted at rest using AES-256.
- Client data may be stored temporarily on local storage accessed by virtual servers but must be deleted when no longer needed.
- Uploaded files are scanned by virus-detection and protection software. Files that do not pass are not stored on any devices.

- Virus protection software is checked for updates at least daily.
- Application-level user activity should be tracked in an auditable manner, typically by storing database records of various user actions. User action records for application users should be retained for the entire time a user is retained on the system.
- The principal of least functionality is to be followed throughout the system, that is, ports, access points, and other capabilities are to be restricted to only what is absolutely necessary.

General Cloud Practices (Amazon AWS)

- Root API Access keys are deleted
- Root access requires MFA.
- Root login should never be utilized unless necessary for actions to be taken.
- There are two Administrator Users. One is for daily use by the system administrator. The other is for backup purposes only.
- Specific, limited IAM Roles should be used for all application-level (API) and other specialized access. These users should only have the privileges required.
- Access Keys for IAM Roles should be rotated annually if there has been any chance of compromise or if there is any change in staff.
- The principal of least privilege should be applied logically and aggressively.
- All system management and configuration options should be logged in CloudTrail logs and retained for at least 180 days in Amazon S3.
- Critical Log Files should be written to CloudWatch for analysis and stored for at least 180 days.
- Cloud-based automated patch management tools (ie AWS Systems Manager – Patch Manager) shall be used to update all systems software and to ensure that critical patches are applied within 72 hours.
- Cloud-based vulnerability scanning tools such as Amazon Inspector and Amazon Guard Duty will be used and results checked on a periodic basis. Guard Duty – which uses AI to analyze traffic shall be checked weekly. AWS Inspector – which scans EC2 instance and other configuration items will be checked quarterly.

Domain Name Service (DNS)

- All HR Avatar DNS configurations should support DNS SEC authentication with an established chain of trust to prevent spoofing.
- All DNS Entries should be reviewed monthly to ensure that no entries point to IP addresses that are not in use by HR Avatar and could potentially point to 3rd party servers (AWS re-allocation)
- The DNS Zone file for all entries will be backed up on a quarterly basis and saved for 2 years.

Virtual Private Networks (Amazon VPC)

- Virtual Private Networks (VPCs) will be used to segregate operational or production systems from non-operational (software testing and company administrative) systems.

- Security Group and Network ACLs should be used to limit traffic to only those ports that are required. If the source/destination IP address can be limited, this information should be incorporated into the security group or NACL as well.

Virtual Servers (Amazon EC2)

- Applications operating on virtual servers should be functionally grouped and co-located on separate virtual servers. (ie: scoring, test admin, test delivery, data reporting, etc).
- All servers will use the most up-to-date version of Amazon Linux (Currently Amazon Linux 2). The servers should use AWS-maintained versions of critical operating software packages such as java, mysql, anti-virus, etc. so that they can be updated to the latest/most up-to-date version regularly. This maintenance shall be via automated systems managers where practical.
- All software that is not maintained up-to-date via Amazon-provided updates (sudo dnf update) must be approved by the Applications Development Manager and the Information Security Manager prior to installation on production systems.
- All servers are checked weekly for available updates to kernel and security applications. Typically, this is accomplished by running “sudo dnf update” each week manually. Note: this practice should be considered a backup to use of automated tools (AWS Systems Manager).
- All servers are rebooted approximately weekly to clear memory leaks and prevent unexpected downtime.
- All servers are monitored for unusual activity.
- All servers should be reviewed annually to ensure all unnecessary software, network services and applications have been disabled/removed.
- Servers that handle file uploads should be equipped with Clam AV anti-virus software that receives daily updates to virus definition files.
- Images (AMIs) are created for each virtual server at least weekly using the Amazon Backup service.
- AMI Images are copied to an alternate region weekly using Amazon Backup.
- All servers with access to client data should be part of the same Virtual Private Cloud (VPC), which is logically isolated from other resources in the cloud and enforces the use of uniquely managed security groups and subnet(s), and the same internet gateway.
- Network Access Control Lists (Network ACLs) should be used to restrict inbound and outbound traffic within all VPCs that transmit proprietary or client data.
- Servers hosting public-accessible websites (www.hravatar.com, sim.hravatar.com, imo.hravatar.com, etc) should have a web application firewall (WAF) attached that contains Web Access Control Lists (Web ACLs) with rules designed to prevent cross-site scripting, denial of service, and sql injection. These Web Application Firewalls can also be used to deny access to black-listed IP Addresses or to cut off high volume users if necessary.
- Servers with access to client data should use a unique security group that is tuned to each specific server, which should restrict access by port, private cloud, and IP address, unless that server requires specific additional port access. Only ports that are absolutely necessary should be opened within the security group.

- Remote administrative logon to servers should only be via secure services such as SSH and SCP and should only utilize public/private key authentication. Password authentication is not permitted for server remote access.
- Remote access to servers is limited to specific source IP addresses allowed via the associated AWS EC2 security group.
- Remote administrative logon to system applications (such as the web server and application server) hosted on the server should only be accessed by HTTPS and allowed only for IP addresses of the known administrative workstation.
- The number of administrative logons (logons that provide application-wide or system-wide access) should be kept to an absolute minimum.
- Passwords used for remote administrative logon to web applications (such as the web server and application server) should be strong passwords, at least 12 characters in length, and changed once per year.
- Server access rights should be assigned to system 'users' using the principle of least privilege (PoLP) which ensures that users do not receive system rights that they do not need to perform their assigned duties.
- Production Firewalls (AWS EC2 Security Groups, VPC Security Groups, RDS Security Groups, Network Access Control Lists and Web Access Control Lists) are configured according to needs/purpose of each specific server and maintained by the Security Manager. Except in emergencies, Security Manager approval is required before any of these production firewall settings may be changed.
- All static content shall be accessed via a Content-Delivery Network where feasible. A web-application firewall should be used to prevent unauthorized access to resources via the content delivery network.
- Load balancers shall route traffic based on Server Name and will not accept traffic that is addressed to an unknown server name.

Log Files

- All servers should be configured to log security-related events generated by the system.
- System log files should be retained locally for a minimum of 60 days to enable post-incident security investigations.
- System log files for the primary HR Avatar server (www.hravatar.com) should be maintained for 180 days via Cloudwatch.
- System log files include: /var/log/secure, /var/log/messages
- System access logs should be retained locally for a minimum of 60 days to enable both security and software bug investigations.
- System access logs for the primary HR Avatar server (www.hravatar.com) should be maintained for 180 days via Cloudwatch.
- System access log files include: /var/log/httpd/ssl_access_log, /var/log/httpd/ssl_error_log
- HR Avatar application log files should be retained locally for a minimum of 7 days to enable both security and software bug investigations.

- HR Avatar application log files for primary HR Avatar server (www.hravatar.com) should be maintained for 180 days via Cloudwatch.
- Vulnerability scanning by Amazon Inspector and Intruder.io on a quarterly basis. Results should be retained for 2 years.

Data Storage (Amazon S3, Amazon Glacier)

- Stored files shall only be accessed via HTTPS.
- Buckets that contain sensitive data (personally identifying information) should be encrypted.
- Data access via the Internet for data files containing sensitive data should be via signed URLs with a short (~15 minutes or less) expiration date.
- Storage of binary files containing personally identifying information (images, audios, and videos) shall not be public and shall require a signed request for access via https.
- During pseudonymization, all binary file data associated with a user is deleted.
- All S3 Buckets that store system-critical and customer data should:
 - Have versioning enabled
 - Replicate to a mirror bucket in the backup region
 - Have either the source or replica backed up via AWS Backup
- Vulnerability scanning by Amazon Inspector on a quarterly basis.

Relational Database (Amazon RDS)

- Database instances should be part of a single Virtual Private Cloud (VPC), which is logically isolated from other resources in the cloud and enforces the use of the same security group and subnet(s), and the same internet gateway.
- Network Access Control Lists (Network ACLs) should be used to restrict network traffic on the database VPC.
- Database access should utilize a security group that restricts access by source IP address and to specific cloud resources within authorized VPCs.
- Remote database access from both applications and ad hoc users must be performed via SSL (TLS 1.2 or higher)
- Passwords used for direct application logon to the databases (from EC2 Servers) should be strong passwords and at least 12 characters in length.
- Passwords used for remote root logon to the databases should be strong passwords, at least 12 characters in length.
- Data files shall be encrypted at rest, including database backups and snapshots.
- Database backups should be automatically run daily.
- At least 3 days of previous database backups should be stored.
- A copy of the database backup should be copied to an alternate region on a weekly basis.
- Automated database backup success should be checked by administrator staff weekly.
- Server-based user privileges should be restricted to functions and databases necessary.

- The database version shall be upgraded promptly when recommended by Amazon AWS, through automated updates within the designated maintenance window.

Production Web Applications

- All production webserver and application server remote administration modules must be accessed via HTTPS (TLS 1.2 or higher) only via authorized workstations only.
- All production web applications that provide access to client data must be accessed via HTTPS only. SSL TLS 1.2 should be required at minimum. Review AWS Recommended security package for SSL in the load balancers annually.
- All production web applications should set the “HTTP Only” and “Secure” cookie attributes on all cookies uses by the application.
- Applications not intended to be operated within a frame shall have the X-Frame-Options header set to prevent display inside a frame to prevent click jacking attacks.
- No passwords should be hard-coded into applications. Where possible, application-level passwords should be stored in encrypted format in the database or in protected files on the server itself.
- During sign-on, applications should show no information confirming a valid username until the user is signed on successfully.
- Applications should display last login and last password change to user after they log in.
- Java applications should utilize standard J2EE persistence practices for database queries and updates.
- Mobile code (javascript) will be restricted via Content Security Policy to HR Avatar and other approved sites only.
- All web Java Applications use native J2EE JSF CSRF protection strategies including randomly generated request-specific view tokens for all POST requests and protected views for GET requests. Non-java applications, if any (there are currently none), should have their own CSRF prevention strategy.
- We applications should use HTTP POST transactions for any requests that show sensitive data, in order to prevent browser caching of sensitive data in temporary client-side folders.
- There should be maximum logical separation between customer or user interaction with applications and administrative access to applications. Different urls, different applications, and different usernames should be utilized to achieve this separation.
- All web applications (internal and external, and including web administrative access to the application) should be developed based on the Open Web Application Security Project Guide (OWASP).
- Session Ids shall not appear in URLs.
- In particular, the following vulnerabilities should be addressed in the software development processes:
 - (i) cross-site scripting (XSS)
 - (ii) injection flaws, particularly SQL injection
 - (iii) malicious file extension

- (iv) insecure direct object references
 - (v) cross-site request forgery
 - (vi) information leakage and improper error handling
 - (vii) broken authentication and session management
 - (viii) insecure cryptographic storage
 - (xi) insecure communications
 - (xii) failure to restrict URL access
- Programming Standards listed in the HR Avatar Software Development Procedures document will be adhered to.
- The OWASP Top Ten vulnerabilities should be review on an annual basis.
- Applications may use non-persistent session cookies that last only as long as a session without requiring the user to log on again.
- Applications may use persistent cookies for auto-logout purposes (username only) from user devices only with permission of the user. These cookies must be configured to expire within 1 year.
- Session inactivation time for non-authenticated users will be no more than 30 minutes. Session inactivation time for authenticated users will be no more than 20 minutes except authoring system users, who are given no more than 60 minutes session inactivation time.
- When a session is inactivated due to inactivity, the web page should automatically forward to an appropriate 'session expired' page.

Corporate Email

- Currently using Google Workspace for corporate email.
- Email should be configured with appropriate DNS and other records to ensure secure emailing.
 - Activate MTA STS and TLS Reporting (policy, and DNS Records)
 - Add DNS SPF Record
 - Add DNS DMARC Record and reject failed emails.
 - Add DNS DKIM Record and enable authentication

System Documentation

- Because it can be used to compromise the integrity off HR Avatar applications, system documentation describing HR Avatar configuration and procedures (ie SW Dev Procedures, Business Continuity Procedures shall be removed from public access and marked as Confidential.
- Any unauthorized or inappropriate attempt to gain access to non-public documentation shall be considered as a security incident and treated accordingly.

Stage and Development Environments

- Live data from production should never be used in sandbox or test environments.
- All system development activities will be performed in specialized development environments which are isolated from the production environment.

- Sandbox activities should never be given access to production data or include production data in analysis or testing.

Vulnerability Scanning

- Annual website vulnerability scanning using Intruder.io
- Developer vulnerability Scanning by SonarQube with all ‘vulnerabilities’ resolved prior to posting any application software to production.
- Identified vulnerabilities must be remediated in a timely manner based on priority. In particular, high and critical vulnerabilities should be remediated within 30 days of identification.

Identifiers

- Information system identifiers can must be logged in the Information System Identifier log and approved by the Application Development Manager.
- The Information Security Manager shall review this log periodically.

Home Office Wireless Networks

- Home office wireless networks used by employees conducting HR Avatar business should use secure access with strong passwords.

Credential and Cryptographic Material Management

HR Avatar systems are accessed by an array of certificates, username/password combinations, access code/key combinations, and multi-factor authentication. Where applicable, these are stored in a password vault in an encrypted format that is only accessible via a single master password.

- Amazon KMS should be used to store, maintain, and regenerate cryptographic keys where practical.
- GoDaddy is a secondary source of certificates and keys.
- Passwords should never be written on hardcopy paper or electronically in unencrypted format.
- Database storage of passwords should always be in encrypted format.
- Amazon Certificate Manager should be used to manage certificates used by HR Avatar applications and applicable cloud services.
- Private keys shall be managed by the Information Security Manager (via KMS).
- Private keys should reside only on computers where they are necessary and within the password vault.

Installation of 3rd Party Software (new 2023)

All new 3rd party software to be installed on HR Avatar production systems must be approved by the Application Development Manager and logged in a software installation log. This log shall indicate approval date and installation date, and it shall be reviewed monthly by the Information Security Manager.

System Logs and Log Retention

In order to be able to reconstruct and investigate potential security breaches, log files from various sources should be generated and stored for an appropriate period. These files should be stored in a format and place where easy access for analysis is possible, and potentially alarms.

HR Avatar uses Amazon AWS CloudTrail and CloudWatch to store critical system and application-generated logs.

AWS Configuration Changes (CloudTrail to CloudWatch)

Critical (admin) Server Instances (EC2 to CloudWatch)

- /var/log/messages
- /var/log/secure
- /var/log/httpd/ssl_access_log
- /var/log/httpd/ssl_error_log
- /application-generated logs (/work/tm2admin5/log etc.)

Data Backup Policy

HR Avatar shall maintain a data backup policy. This policy is contained within the Business Continuity Plan. In general, both the production database and file storage are backed up daily. The database is backed daily up to Amazon S3 (RDS Snapshots) and copied to the backup AWS region weekly.

For all buckets that store system critical data and files, or customer files, S3 versioning is used with appropriate periods for deletion of non-current versions. For these same buckets, file storage (S3) is replicated to mirror buckets in the backup region in real time and these mirror buckets are backed up weekly using AWS Backup.

Data Sharing with API Users

Both HR Avatar clients (end users) and partners can access the HR Avatar API.

While HR Avatar API Users are able to access only data contained within their specific client or partner accounts, it is important that provisions be made for protection of this data once it leaves HR Avatar control. To ensure the protection of this data, HR Avatar will establish data sharing agreements with all new parties that access the API during the initial contracting process and all existing partners / clients who access the API during 2019 or afterward.

The standard draft data processing agreements for partners and clients are available upon request.

Starting in 2023, a Partner Security Questionnaire will be used to ensure appropriate controls are in place for all partners who access the HR Avatar API. The Information Security Manager will maintain a log of all partners and ensure that the questionnaire is administered annually.

Incident Response

When a security incident is reported, regardless of how insignificant it may seem, it must be logged in the incident log includes in Appendix A.

Additional incident response procedures are detailed in the *HR Avatar Security Incident Response Guidelines*, which is maintained by the Security Officer. These guidelines are contained in Appendix B.

Housekeeping Log

A log of all IT Housekeeping and other relevant activities will be maintained and kept up to date. This log will be reviewed by the President at least monthly to ensure compliance with requirements specified in this and other related documents.

Audit and Review

SOC Audits

HR Avatar applications currently touch or store zero financial information for HR Avatar or HR Avatar's clients. As of the time this report was published, HR Avatar has not conducted any SOC audits. We do, however, recognize the value of a SOC 3 audit, since this provides the appropriate level of assurance regarding our processes and internal controls given the nature of the data we store. Finally, we often share the SOC reports generated by our primary cloud services provider (Amazon AWS).

Inspection Scans and Auditing

HR Avatar will make maximum use of the automated security inspection scanning tools.

- Network and site activity is monitored by Amazon Guard Duty and checked continuously.
- EC2 instances and S3 buckets are checked quarterly with Amazon Inspector.
- Application code is scanned with SonarQube and all vulnerabilities are resolved prior to posting to production.
- Annual Website Vulnerability Scanning / Automated Penetration Testing via Intruder.io

Website Vulnerability (Penetration) Testing

HR Avatar conducts periodic formal 3rd Party penetration testing to verify the strength of its practices and identify deficiencies proactively. The most recent annual penetration test was performed in March 2024. A report is available upon request proving that all deficiencies have been satisfactorily addressed.

We also cooperate with clients and partners who wish to perform penetration testing as a part of their own procedures. Noted deficiencies are taken seriously and acted upon quickly.

HR Avatar also performs annual network vulnerability scanning with Intruder.io.

Identified vulnerabilities must be remediated within the appropriate timeframe depending on severity. High and critical vulnerabilities should be remediated within 30 days.

Periodic Internal Risk Assessment

Per the HR Avatar Risk Assessment Process (separate document) a risk assessment should be conducted by management at least annually.

Quarterly User Access Rights Review

All system and application users with administrative access rights shall be reviewed at least quarterly to improve/enforce the principal of least privilege and ensure that no users are granted inappropriate access rights. This includes both logons (username/passwords) used for interactive access as well as access keys used for application-oriented access.

Data Privacy Framework Program

HR Avatar is self-certified and listed as an active participant in the Privacy Shield program (<https://www.dataprivacyframework.gov/>) for the **EU-U.S. Data Privacy Framework**.

Appendix A: Security Incident Log Format

This log shall be maintained by the Information Security Officer. A copy of this log can be made available to any HR Avatar executive, any employee, or client upon request.

The log will utilize the following format:

Id	Date	Incident Description	Severity	Incident Report Completed

- Severity Levels: High: Did or could have impacted customers. Medium: Could have led to actions that could impact customers. Low: Easily corrected, minor impacts if any.

Appendix B: Incident Response Procedures

For each logged incident, an incident report will be documented by the Incident Response Officer and filed for audit and review. The incident report will cover the following:

Section	Task	Notes
1	Describe the incident	Time, Date, all other known details
2	Describe the impact on customers	
3	Identify the cause of breach	
4	List actions taken / planned to prevent future occurrences	
5	List actions taken / planned to recover from this occurrence.	

Appendix C: Employee Termination Checklist

HR Avatar Employee Termination Checklist - Security

Employee: _____

Termination Date: _____

Date	Action
	Disable employee Google Workspace business applications account access (email, drive, etc), assign data to appropriate current employee for up to 60 months. Typically the email is shifted to become an alias for another employee for 6 months – 1 year.
	Disable employee Dialpad account access (phone, web conferencing).
	Disable employee access to HR Avatar operational systems.
	If applicable, change all operational system root user passwords.
	Collect all HR Avatar hardware/software issued while employed.
	Disable Hubspot Access.

Appendix D: Client Account Termination Checklist

1. Comply with all specific contractual requirements concerning termination.
2. Place account in a “disabled” status.
3. Review pseudonymization settings to ensure that full pseudonymization of all data in the closed account occurs within 12 months.
4. Review data retention settings to ensure that data is retained for no longer than 3 years so that it is deleted. If faster deletion is desired by the client, change the setting to match client desires.

Appendix E - Prohibited Software and Hardware

HR Avatar staff are prohibited from installing any of the following prohibited software applications on HR Avatar-provided systems:

None. Note that all SW installation on HR Avatar Stage and Production systems must be approved by the Applications Development Manager.

Appendix F: Overview of the Production Infrastructure

Removed (4/2023). All architecture and systems documentation is now marked as Confidential and is not available via the website. Please request from the Information Security Manager or the Applications Development Manager.

Appendix G: Summary of Recurring Requirements

Item	Periodicity	Notes
Annual Document Review by ISM	Annual	Includes a report of review for record-keeping purposes. Performed by Information Security Manager.
Annual Security Training and Document Review	Annual	Signed forms collected and retained from each employee.
Annual Report	Annual	Information Security Manager
Security Review Discussion	Monthly	President and Information Security Manager
Review Identifier Log	Monthly	President
Review Software Installation Log	Monthly	President
Review Housekeeping Log	Monthly	President

Appendix H: Version History

Version	Date	Changes	Approved By & Date
Version 1.0	7/23/2018	Initial release	
Version 1.01	8/30/2018	Enhancements to practices incorporated.	
Version 1.02-04	9/2018	Enhancements initiated after PCI checklist review.	
Version 1.05	1/11/2019	Enhancements per January Security Assessment	
Version 1.06	1/20/2019	Misc. enhancements following completion of several corporate security checklists.	
Version 1.07	2/12/2019	Periodic review and update.	
Version 1.08	3/7/2019	Periodic review and update.	
Version 1.09	4/18/2019	Periodic review and update.	
Version 1.10	7/12/2019	Periodic review and update.	
Version 1.11	8/25/2019	Periodic review and update.	
Version 1.12	3/16/2020	Periodic review and update.	
Version 1.13	1/29/2021	Periodic review and update.	
Version 1.14	2/10/2021	Periodic review and update.	
Version 1.15	3/14/2021	Periodic review and update.	
Version 1.16	3/17/2022	Periodic review / update. Added code scanning requirements.	
Version 1.17	4/28/2022	Revised log retention requirements.	
Version 1.18	9/2022	Misc updates	
Version 1.19	4/1/2023	Periodic review and update. Added vulnerability scanning requirements. Other revisions per review by Blue Cross Blue Shield (Keylight)	
Version 1.20	4/23/2023	Change of Information Security Manager to Michael Russiello	
Version 1.21	12/16/2023	Change of Information Security Manager to Sandy Stiltz, Application-level accounts. Revised monthly	

		reporting requirements. General edits for readability. Added Sentino.io for text analysis.	
Version 1.22	4/2024	Revision to password rules. Change Privacy Shield to Data Privacy Framework. Other minor edits – review.	
Version 1.23	6/2024	Establishment of the Interim Information Security Officer. Added Approval of all changes	M. Russiello, 6/2/2024
Version 1.24	6/2024	Added requirement to review the Risk Assessment Process and Risk Identification Worksheet with all employees during annual training.	M Russiello, 6/5/2024
Version 1.24.1	6/2024	Updated password requirements for users with system administrative access	M Russiello 6/19/2024
Version 1.24.2	7/2024	Revised transmittal letter to include explicit approval of the revision and date of signature.	M Russiello 7/29/2024
Version 1.24.3	8/2024	Modified the application user definitions.	M Russiello 8/28/2024
Version 1.24.3	8/2024	Revised transmittal letter to include explicit approval of the revision and date of signature.	M Russiello 8/28/2024
Version 1.25.1	12/2024	Updated dates. Removed # from password rules (not allowed). Changed Intruder.io to an annual scan. Added requirement to backup DNS Zone file Quarterly. Added use of Amazon Backup for automated backup of resources.	M Russiello 12/20/2024
Version 1.25.1	4/2025	Changed logo Added In-person interview requirement Added automatic user disablement feature for account users Added Unusual Logon Policy	M Russiello 4/9/2025
Version 1.26.1	3/2026	Added requirement for all system admin logons to use MFA.	M Russiello 3/26/2026
Version 1.26.2	4/2026	Added a Generative AI Usage Policy to the Employee Responsibilities Section	M Russiello 4/5/2026
Version 1.26.3	4/2026	Added requirement for public S3 buckets to require HTTPS. Revised S3 Backup procedures to use versioning of objects with appropriate expirations for non-current versions, real-time replication to the back-up region, and use of AWS Backup for additional backups on a weekly basis.	M Russiello 4/28/2026

Appendix I: Security-Specific Programming Standards

Removed from this manual and incorporated into Software Development Procedures (controlled document).

Please refer to the HR Avatar Software Development Procedures.