

ENGAGEX® ENTERPRISE USERS SECURITY OVERVIEW



EFFECTIVE DATE: NOVEMBER 20, 2025

SECURITY AT ENGAGEX

EngageX® is an AI powered coaching platform for public speaking, presentations, pitching and customized speech training. Because you trust us with sensitive audio and performance data, we treat security, privacy, and reliability as core product features, not afterthoughts.

This Security Overview explains how we protect your data, how long we keep it, and what controls you have when using EngageX®.

We follow three principles:

1. Minimize data: collect only what is needed to deliver AI powered coaching.
2. Protect by design: use encryption, access controls, and hardened cloud infrastructure.
3. Respect your control: give you clear options for access, deletion, and safe export.

WHAT WE COLLECT (AND WHY)

To run EngageX® and deliver AI driven feedback, we may process the following:

Personal Information

- Name
- Email address

NOTE: EngageX® is not designed for primary use on a company's private network and is optimized to operate on personal mobile devices such as iPads, smartphones, and personal computers.

- Audio input from your speaking sessions
- AI analysis and feedback metrics such as impact score, trigger words, pace, clarity, and filler words

We use session data exclusively to:

- Generate AI feedback on your performance
- Allow you to download your recording for personal review
- Improve the accuracy and quality of EngageX® features

Usage Information

- Browser type and version
- Interaction data such as which features you use

We use this to:

- Keep the platform stable and performant
- Understand feature usage
- Detect abuse and maintain security



DATA RETENTION AND DELETION

We intentionally limit how long we retain your session content:

- For our Presentation Mastery or Pitch sessions, all uploaded PowerPoint/slides files are deleted immediately upon session completion, and **we do not retain or store any user-provided materials.**
- Session recordings and related data are automatically deleted within 24 hours of creation, unless you choose to download them.
- Once downloaded to your own device or storage, you are responsible for protecting those copies. EngageX® cannot control or secure files stored outside our platform.
- You can request access to or deletion of your stored personal information, such as your profile details and account data, subject to our legal and operational obligations.

This short retention window is designed to reduce risk while still letting you review and learn from your sessions.

HOW ENGAGEX PROTECTS YOUR DATA

We combine application level safeguards with cloud infrastructure security to protect your data throughout its lifecycle.

1. Encryption

- In transit:
 - All data exchanged between your browser and EngageX® is protected using HTTPS and TLS encryption.
- At rest during the short time we store it:
 - Session storage and media files are encrypted using AES encryption standards that align with modern practices for securing sensitive data.

2. Authentication and Access Controls

- EngageX® uses Django built in authentication with securely hashed passwords, reducing risk if credentials are ever exposed.
- EngageX® supports two-factor authentication to ensure secure and protected user login.
- Role based access control ensures only authorized roles can access sensitive features or data, such as admin functions or operational logs.
- Internally, access to production systems and data is restricted to a small number of authorized team members, following least privilege principles.



3. Application Security

We apply a secure by default mindset informed by the defense in depth approaches of leading SaaS security programs.

Key protections include:

CSRF protection: Django token based CSRF protection is enabled to reduce cross site request forgery risks.

Input validation: File uploads and user inputs are validated rigorously to limit injection and file based attacks.

Secure media access:

User uploaded media in cloud storage is accessed via pre signed URLs, which provide time limited and scoped access tied to your session or account.

CLOUD INFRASTRUCTURE AND NETWORK SECURITY

EngageX® is hosted on Amazon Web Services, leveraging their hardened and widely adopted infrastructure.

- Databases are placed in a private VPC subnet, isolated from direct public internet access.
- AWS Security Groups are configured to allow only the minimal inbound and outbound traffic required for the platform to operate.
- We rely on AWS underlying security controls and certifications, including SOC 2 and ISO 27001, for physical and infrastructure level protection of the environment where EngageX® runs.

In addition, we maintain:

- Continuous monitoring and logging through AWS CloudWatch, GuardDuty, and CloudTrail for:
 - Threat detection and anomaly alerts
 - Access and change auditing
 - Forensic investigation support in case of incidents

PLATFORM SECURITY, RISK MANAGEMENT AND YOUR CONTROLS

EFFECTIVE DATE: NOVEMBER 20, 2025

SECURITY MONITORING, DETECTION AND RESPONSE

Even as a focused, specialized product, EngageX® treats security events as critical operational concerns.

We use AWS native tools such as:

- CloudWatch for infrastructure and application metrics and alerts
- GuardDuty for threat detection at the AWS account and network level
- CloudTrail for detailed audit logs of API calls and configuration changes

These logs and alerts help us:

- Spot unusual patterns such as suspicious access attempts
- Investigate and respond quickly to potential incidents
- Maintain an auditable trail of important security relevant actions

If we identify a security incident that materially impacts your data, we will:

1. Investigate and contain the issue
2. Remediate the underlying cause
3. Notify affected users where appropriate and as required by law

CYBERSECURITY INSURANCE AND RISK MANAGEMENT

In addition to technical and organizational controls, **EngageX® maintains dedicated cybersecurity insurance coverage.**

This insurance:

- Acts as a financial backstop in the event of qualifying security incidents
- Reflects our commitment to treating security as a managed business risk, not just a technical problem
- Complements, but does not replace, our responsibility to prevent, detect, and respond to security threats as effectively as possible

This is one more layer in a broader risk management strategy that includes data minimization, short retention, strong encryption, and hardened cloud infrastructure.

PRIVACY, COMPLIANCE AND DATA RIGHTS

EngageX® security practices are tightly aligned with our Privacy Policy, effective November 20, 2025, which describes in detail:

- What personal data we collect
- The legal and operational purposes for which we use it
- Your rights to access and request deletion of your data

Our approach is to:

- Limit data collection to what is necessary for AI coaching and platform operations
- Maintain transparency about retention periods and how session recordings are handled
- Respect reasonable data subject requests, subject to legal requirements



DATA SHARING AND THIRD PARTY ACCESS

EngageX® **does not sell your personal information.** We only share data in limited circumstances, such as:

1. Legal and regulatory obligations
 - When we are required to respond to lawful requests from government bodies, regulators, or law enforcement.
2. Fraud prevention and security monitoring
 - When necessary to protect the platform, users, or the public from security threats, fraud, or abusive behavior.
3. Cloud and infrastructure providers
 - We run on AWS and may use other vetted infrastructure or analytics providers to host, process, or secure EngageX®. Any such providers are bound by contractual and technical controls.

We do not grant unrestricted access to customer data to third parties for advertising or unrelated purposes.

YOUR RESPONSIBILITIES AND BEST PRACTICES

Security is a shared responsibility between EngageX® and our users.

You can help keep your account and data safe by:

- Choosing a strong, unique password for EngageX®
- Keeping downloaded recordings in secure locations such as encrypted drives or private cloud folders
- Avoiding sharing your recordings or feedback reports publicly unless you are comfortable with that exposure
- Promptly contacting us if you suspect unauthorized access to your account

Remember:

Once a session recording is downloaded, EngageX cannot protect that copy. Treat it as you would any sensitive performance or training material.

CONTACT AND SECURITY QUESTIONS

If you have questions about EngageX® security or need to report a potential issue, you can reach us at:

Email: Info@engageXai.io