Privacy Policy

Last Updated: November 2nd, 2025

At AIncident, we take your privacy seriously. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our incident reporting and management platform. We never sell your personal data.

1. Information We Collect

Personal Information

When you create an account, we collect:

- Name and email address
- Phone number
- Organization and location details
- Payment information (processed securely by Stripe)
- Job title and role assignments
- Employee identification information (as required for security personnel)

Incident Report Data

When you use our service, we collect:

- Voice recordings and audio files (via Twilio)
- Text-based incident reports and descriptions
- Photos and images related to incidents
- Location data and GPS coordinates
- Date, time, and location information
- User actions and incident updates

Automatically Collected Information

We automatically collect:

- Login and authentication data
- Device information (browser type, operating system, device identifiers)
- IP addresses and general location
- How you use our service (features accessed, actions taken)
- Technical logs for security and troubleshooting

Analytics

We use Google Analytics to understand how visitors interact with our website and improve user experience. You can opt out of analytics tracking by using browser privacy settings or ad blockers.

Free Trial Information

If you sign up for a free trial:

- We collect payment information at signup (credit card details processed by Stripe)
- We track your trial start and end dates
- We monitor usage during the trial period

- We send automated notifications about trial status
- Your payment method will be charged automatically if you don't cancel before trial expiration

2. How We Use Your Information

We use your information to:

- Provide and maintain our service
- Process and route incident reports to the right people
- Generate AI summaries of incident reports
- Convert voice recordings to text
- Track and map incident locations
- Manage user accounts and permissions
- Send notifications and alerts
- Process payments and prevent fraud
- Provide customer support
- Send important updates about your account
- Improve our service through analytics
- Comply with legal obligations
- Administer free trials and convert to paid subscriptions
- Send trial expiration reminders and billing notifications

3. AI and Voice Processing

AI-Powered Summaries

We use OpenAI's API to create summaries of your incident reports. When you submit a report, the content is sent to OpenAI for processing. OpenAI has a zero data retention policy, which means:

- Your data is not used to train their AI models
- Your data is deleted within 30 days
- OpenAI is contractually required to protect your data

In the future, we may develop our own AI models. If we do, we'll update this policy and give you clear choices about how your data is used.

Voice Recording and Processing

Voice recordings work this way:

- Processed by Twilio for call routing
- Stored in secure AWS S3 storage for up to 3 years
- Converted to text transcripts using Twilio's technology
- Available for Admin users to download through our platform
- Text transcripts are kept for 7 years

Voice recordings are sensitive, so we protect them with strong security measures. Admin users in your organization can access and download voice recordings for legitimate business purposes like incident review, training, and quality assurance.

4. Data Storage and Security

Where Your Data is Stored

- All data is stored on Amazon Web Services (AWS) in the United States
- Primary storage is in the AWS us-east region
- We plan to expand to AWS us-west region
- We are SOC 2 compliant for data security
- Access is controlled through AWS security systems

How We Protect Your Data

We use industry-standard security measures including:

- Encryption when data is transmitted over the internet
- Encryption when data is stored on our servers
- Multi-factor authentication for Admin accounts
- Role-based access controls (only authorized people can access specific data)
- Regular security checks and vulnerability testing
- Secure backups with 7-day retention
- Monitoring and logging of system access

No security system is 100% secure, but we work hard to protect your information using the best available methods.

5. Third-Party Services

We use these trusted partners to operate our service:

- **AWS (Amazon Web Services):** Cloud storage and hosting
- **Stripe:** Payment processing for subscriptions
- **Twilio:** Voice call processing and routing
- **OpenAI:** AI-powered incident summaries
- **Google Analytics:** Website usage analytics
- **GoDaddy:** Domain hosting

Each service has its own privacy policy. We only share the minimum data necessary for them to provide their services. These partners are required by contract to protect your data.

6. Who Owns Your Data

Account Structure

AIncident has three types of users:

- **Admin Users:** Create the account, manage everything, and own all data
- **Manager Users:** Oversee specific locations within the organization
- **Standard Users:** Create and submit incident reports

Important: Data Belongs to the Organization

All incident reports, voice recordings, and related data belong to the Admin's organization, not to individual users who created them. This means:

- If a Manager or User leaves your organization and deletes their account, their incident reports stay with the organization
- Only the Admin can delete organizational data
- Individual users can only delete their personal login information (name, email, password)
- The Admin always retains access to all incident data

This structure ensures your organization doesn't lose important incident records when employees leave.

7. Data Sharing

We do not sell, trade, or rent your personal information. We only share your information:

- **With your consent:** When you explicitly authorize sharing
- **With service providers:** The partners listed above who help us operate the service
- **To comply with the law:** When required by court order or legal obligation
- **To protect rights and safety:** To enforce our terms, prevent fraud, or protect users
- **In business transfers:** If we merge with or are acquired by another company

8. Your Rights

You have these rights regarding your personal data:

- **Access:** Request a copy of your data
- **Correction:** Update inaccurate information
- **Deletion:** Request deletion of your account (subject to organizational ownership rules)
- **Portability:** Receive your data in a machine-readable format
- **Opt-out:** Unsubscribe from marketing emails
- **Review:** Ask how we process your data

California Residents

If you live in California, you have additional rights under the California Consumer Privacy Act (CCPA):

- Right to know what personal information we collect and how we use it
- Right to request deletion of your information
- Right to opt out of sale of your information (we don't sell data)
- Right to non-discrimination for exercising your rights
- Right to correct inaccurate information

How to Exercise Your Rights

Submit a request through our contact form at [contact URL] or email [support email]. We'll respond within 30-45 days.

We may need to verify your identity before processing your request. If you're a Manager or User within an organization, you cannot request deletion of incident reports you created because those belong to your organization's Admin.

9. Voice Recording Access and Consent

Admin Access to Voice Recordings

Admin users can access and download voice recordings from their organization. This access is for legitimate purposes like:

- Reviewing incident details
- Quality assurance
- Training staff
- Compliance requirements

Important for Organizations: If you're an Admin user, you must inform your Managers and Users that their voice recordings may be accessed by administrators. You should:

- Get appropriate consent from employees before they start recording
- Tell them that admins can access their recordings
- Comply with employment laws and recording consent requirements
- Use voice recordings only for proper business purposes
- Keep recordings confidential

AIncident provides the technical ability for admins to access recordings, but you are responsible for following all applicable laws about recording consent and employee privacy.

10. Data Retention

How Long We Keep Your Data

We retain different types of data for different periods based on legal requirements, business needs, and industry best practices.

Active Accounts

While your subscription is active:

- **Incident reports and text data:** 7 years from creation date
- **Voice recordings:** 3 years from creation date
- **Text transcripts of voice recordings:** 7 years from creation date
- **Account information:** Duration of your active subscription
- **Payment records:** 7 years (required for tax and legal compliance)

Free Trial Accounts

During and after a free trial:

- **Trial data:** All data created during the trial is retained according to the same retention periods as active accounts
- **If trial converts to paid:** All trial data carries over seamlessly

- **If trial is cancelled:** Data is retained for 7 days after cancellation, then permanently deleted
- **Payment information:** Stored securely by Stripe from the moment you enter it at trial signup

Industry-Specific Retention Requirements
Important Notice: The retention periods listed above are AIncident's standard retention policies. However, your organization may be subject to different retention requirements based on:

Your Industry:
- Security services companies may have state-specific incident log retention requirements
- Healthcare organizations subject to HIPAA may need longer retention periods
- Government contractors may have federal retention requirements
- Financial services may have SEC or other regulatory retention rules
- Educational institutions may have specific records retention policies

Your Jurisdiction:
- State laws may require longer (or shorter) retention periods
- Local regulations may impose additional requirements
- Contractual obligations with your clients may dictate retention periods

Your Responsibility: You are solely responsible for:
- Understanding retention requirements applicable to your business
- Exporting and maintaining data according to your legal obligations
- Ensuring AIncident's retention periods meet your needs
- Implementing additional archival or retention systems if required
- Consulting with legal counsel about your specific retention obligations

If AIncident's default retention periods don't meet your requirements, you should export and archive data separately to ensure compliance with your applicable laws and regulations.

Deleted Accounts
When an Admin deletes their account:
- Access is immediately removed
- Login credentials are immediately deleted
- All data is deleted from active systems right away
- Backup data is automatically removed within 7 days
- Payment records may be kept longer for legal compliance
- Anonymized analytics data may be kept for business insights

When a Manager or User deletes their account:
- Their personal information (name, email, login) is deleted
- Their incident reports stay with the organization
- The Admin keeps full access to all data

11. Children's Privacy

AIncident is for adults 18 and older. We don't knowingly collect information from anyone under 18. If you think we've collected information from someone under 18, please contact us immediately at [support email] and we'll delete it.

12. International Data Transfers

Your information is stored and processed in the United States. If you're using AIncident from another country, your data will be transferred to the U.S. Data protection laws may be different in the U.S. than in your country.

By using our service, you consent to this transfer. We use trusted partners and security measures to protect your data regardless of where it's processed.

13. Do Not Track

Some browsers have a "Do Not Track" feature. We don't currently respond to Do Not Track signals because we only use essential cookies for login and security. If an industry standard for Do Not Track is established, we'll update our practices accordingly.

14. Changes to This Policy

We may update this Privacy Policy from time to time. When we do:

- We'll post the updated policy on our website
- We'll update the "Last Updated" date at the top
- For material changes, we'll email the Admin address on file at least 30 days before the changes take effect

Your continued use of the service after changes take effect means you accept the updated policy. If you don't agree with changes, you can stop using the service and close your account.

15. Data Breach Notification

If we discover a data breach that affects your personal information, we'll notify you without undue delay. Our notification will include:

- What happened and what information was affected
- Steps we're taking to address the breach
- What you can do to protect yourself
- How to contact us with questions

We follow all applicable laws for data breach notification, including California law requirements.

16. Contact Us

If you have questions about this Privacy Policy or want to exercise your privacy rights, contact us:

AIncident Privacy Team
Email: privacy@aincident.io
Contact Form: https://aincident.io/contact

For California residents, you can also use this contact information to request details about our compliance with California privacy laws.
