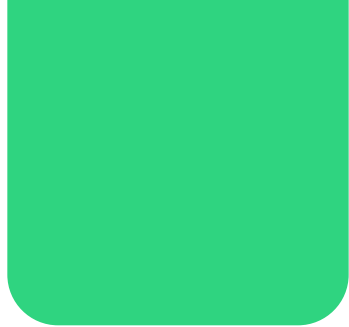




Amira's Safety by Design (SbD) Protocols



OVERVIEW

In an era of unprecedented digital connectivity, school districts face the dual challenge of leveraging technology for learning while safeguarding students from emerging online threats and escalating mental health crises. The digital environment, while rich with educational opportunity, can also be a venue for bullying, harassment, and expressions of despair that signal a student's potential for self-harm or violence toward others. Recognizing this, educational leaders require sophisticated, reliable, and ethically designed tools to help identify and support at-risk students before a crisis occurs.

These brief details the architecture, design principles, and compliance framework of Amira SbD. Amira SbD is engineered to provide school officials with timely, actionable intelligence derived from student interaction with Amira, the AI Teacher's Assistant. SbD does not replace the professional judgment of educators, counselors, and administrators, but flags critical warning signs that might otherwise be missed.

Updated: 6/24/2025

Proactive Prevention Through Safety By Design (SbD)

Amira SbD is governed by a set of core design principles that embed safety, privacy, and fairness into every layer of the technology and its operation. These principles ensure that our commitment to protecting children is proactive, comprehensive, and respectful of their rights.

Amira Safety by Design (SbD) mandates that the burden of safety must not fall solely upon the end-user—in this case, students and school staff.⁶ Amira SbD assumes service provider responsibility by proactively anticipating and engineering out potential for harm and misuse. This is a holistic approach that considers safety across the entire product lifecycle, from initial conception through development, deployment, and ongoing maintenance.

Our implementation of SbD includes several key practices:

- **Accountability:** We nominate specific internal teams who are accountable for the creation, evaluation, and implementation of all user safety policies and operational procedures.
- **Documented Risk Management:** Before deploying new features, we conduct documented risk and impact assessments to evaluate and remediate any potential online harms that could be facilitated by the product.
- **Clear Protocols:** We maintain clear internal protocols for engaging with law enforcement and external mental health support services, ensuring that when a critical threat is identified, the escalation path is swift and effective.
- **Continuous Vigilance:** The digital landscape and the language students use are constantly evolving. Our safety framework includes continuous monitoring of emerging threat patterns and regular updates to our detection systems to ensure they remain effective over time.

Foundational Privacy

Complementing our commitment to safety is an equally rigorous adherence to Privacy by Design, a framework for embedding data protection into the fundamental design of technology. This approach ensures that our platform can achieve its safety objectives without compromising student privacy. The system is built upon the seven foundational principles of Privacy

- 1. Proactive, Not Reactive:** Privacy safeguards are not bolted on as an afterthought; they are integral to the system's architecture, designed to prevent privacy infractions before they can occur.
- 2. Privacy as the Default Setting:** The platform is configured with the highest privacy settings by default. No action is required from a school or a student to be protected; privacy is automatic. This aligns with global best practices, such as the UK's Age Appropriate Design Code, which mandates high privacy settings for services likely to be accessed by children.
- 3. Privacy Embedded into Design:** Privacy is an essential component of the core functionality. This is achieved through strict adherence to data minimization (collecting only the data necessary for the stated purpose), purpose specification (using data only for the explicit purpose of student safety), and collection limitation.
- 4. Full Functionality (Positive-Sum):** The platform is engineered to demonstrate that robust safety and strong privacy are not mutually exclusive. It is possible to achieve both without trade-offs.
- 5. End-to-End Security:** Strong security measures protect data throughout its entire lifecycle, from secure collection via authorized APIs to secure storage with encryption and, finally, to secure and timely destruction as defined by district policy.
- 6. Visibility and Transparency:** The platform's operations and data handling practices are transparent and subject to verification by our partner school districts, fostering trust through openness.
- 7. Respect for User Privacy (User-Centric):** The system is designed to serve and protect the individual student, making their privacy and well-being the central focus.

Commitment To Ethical And Unbiased AI

Amira SbD acknowledges the critical concerns raised by privacy advocates regarding the potential for monitoring technologies to reinforce existing societal biases, leading to disproportionate disciplinary actions against marginalized student populations. Our commitment to ethical AI is a core component of our design philosophy, and we employ multiple strategies to mitigate the risk of bias.

Our model development process includes comprehensive safety testing and "red teaming" exercises specifically focused on child safety scenarios to identify and correct potential biases before deployment. Furthermore, our Natural Language Processing (NLP) models are intentionally designed to move beyond simplistic keyword flagging, which is a known source of bias. The system is trained to understand context and dialectical variations, such as African American Vernacular English, to reduce the likelihood of misinterpretation that could unfairly flag non-threatening communication. This focus on linguistic nuance is essential for building a system that is both effective and equitable.

Architecture For Detecting & Reporting Danger

The platform integrates exclusively with school-managed digital environments, such as Clever and Classlink. Amira only monitors when a student is actively engaged in the Amira app. There is no passive listening. No data is collected unless a student is logged in and in an active session.

Data is accessed via secure, authorized Application Programming Interfaces (APIs) with narrowly defined permissions. This method ensures that the platform only accesses the data necessary to perform its function, in strict accordance with the principle of data minimization.

This relationship is governed by a formal contract that establishes Amira SbD as a "school official" with a "legitimate educational interest" under the FERPA school official exception, legally binding the platform to act as an extension of the school and adhere to all FERPA requirements.



Secure, Segregated Cloud Processing Environment

All data processing occurs within a highly secure, multi-layered cloud environment (Amazon Web Services) that employs industry-best security practices.

- 1. Encryption:** All student data is protected with strong encryption protocols. Data is encrypted in transit using Transport Layer Security (TLS) 1.2 or higher and encrypted at rest using the Advanced Encryption Standard (AES) with 256-bit keys.
- 2. Logical Segregation:** Each school district's data is maintained in a logically segregated and isolated environment. This architectural control prevents any possibility of data being shared or co-mingled between different school districts.
- 3. Third-Party Validation:** The platform's infrastructure and operational controls are regularly audited against recognized industry standards, including SOC 2 (Service Organization Control 2). This provides independent, third-party verification that our security practices meet a high standard of excellence and align with frameworks like those promoted by NIST.

Configurable NLP for Identifying Danger Signals

The core of the Amira SbD platform is its advanced Natural Language Processing (NLP) engine. This engine is designed to accurately identify genuine signals of potential harm by understanding the context and intent of language, a significant advancement over legacy systems that rely on simple and often inaccurate keyword matching.

Step 1: From Raw Voice/ Text To Actionable Mark-Up

When voice or text is collected from a student's interaction with Amira, raw inputs are converted into a standard marked-up text block. This block is in turn passed through a multi-stage analytical pipeline. This pipeline is inherent in Amira's baseline capacity to interact with, dialog with, and tutor the student.

- 1. Data Preprocessing:** The text is first cleaned and standardized. This involves tokenization (breaking text into individual words or tokens), lemmatization (reducing words to their root form), and normalization to handle the slang, abbreviations, misspellings, and emojis common in student communication.
- 2. Feature Extraction:** The preprocessed text is then converted into a numerical representation that machine learning models can understand. The platform uses sophisticated techniques like word embeddings, which capture the semantic relationships and contextual meaning of words.
- 3. Model Analysis:** Processed text then is ingested into a range of AI models that perform analysis like Reading Error Detection. Some of these models.

Step 2: ML Threat Identification

The platform does not rely on a static, pre-defined list of "danger words." Such an approach is brittle and easily circumvented. Instead, the system's AI models are trained on a vast and diverse dataset of language, enabling them to recognize evolving slang, code words, and obfuscation techniques that students may use to hide their intent.¹⁸ The models are also designed to detect shifts in an individual's language patterns and sentiment over time, which can be a powerful early indicator of a developing mental health crisis. In step 2, the Threat Model identifies a potential danger signal.

Step 3: District-Level Customization

Recognizing that each school community is unique, the platform allows authorized administrators to “delist” or “up-weight” alert categories based on their local safety policies and priorities. This ensures the system is aligned with the district's specific intervention strategies. Threats from Step 2 are evaluated against the SEA/LEA weightings. A Threat is then green-lit for notification or red-lit. The use of advanced, contextual NLP is not just a technical feature; it is a critical tool for ethical operation and risk mitigation. Simple keyword-flagging systems are notoriously prone to error, often misinterpreting academic research on sensitive topics (e.g., a student searching for information on LGBTQ+ issues) or culturally specific dialects as threats. This can lead to disproportionate scrutiny for marginalized students and create a chilling effect that discourages legitimate academic inquiry. The platform's reliance on contextual NLP is a direct response to these documented harms. By analyzing intent, the system can differentiate between a student expressing suicidal ideation and one analyzing a character in literature, thereby protecting both student safety and academic freedom. This nuanced approach, combined with a final layer of human moderation for the most severe alerts, dramatically reduces the rate of false positives, ensuring that educators' valuable time is spent responding to genuine needs rather than chasing erroneous flags.

Architecture for Notification

Identifying a potential threat is only the first step; an effective response depends on delivering clear, actionable information to the right people at the right time. The Amira SbD platform features a robust and highly configurable notification architecture designed to initiate and support a coordinated incident response.

Tiered Alerting And Role-Based Routing

The platform automatically categorizes every potential threat by severity level, which can be customized by the district. For example:

- **Tier 1 (Critical):** Imminent threat to life (e.g., explicit suicidal ideation, planning of violence).
- **Tier 2 (Serious):** Significant risk indicators (e.g., severe bullying, hate speech, self-harm).
- **Tier 3 (Concern):** Policy violations or lower-level concerns.

Each tier is linked to a notification workflow defined by the SEA/LEA.²¹ A Tier 1 alert can be configured to immediately notify the district's entire crisis response team—including designated administrators, counselors, and school resource officers—simultaneously. In contrast, a Tier 3 alert might be routed only to a specific school's principal or dean of students. This tiered system ensures that the response is proportional to the threat and that personnel are not overwhelmed with irrelevant information.

Delivery and Response Confirmation

Alerts are pushed onto whatever messaging platform is configured. The platform also features a "closed-loop" acknowledgement system. When an alert is sent, recipients are required to acknowledge that they have received it and are taking action.

Compliance with Federal Student Privacy Laws

Amira SbD is fully committed to upholding all federal laws governing the privacy and security of student data. The platform's architecture, policies, and contractual agreements are designed to ensure strict compliance with FERPA, COPPA, and CIPA.

Family Educational Rights and Privacy Act (FERPA)

Compliance with FERPA is a cornerstone of the platform's design. The relationship with each school district is structured to meet the requirements of the "school official" exception to FERPA's general consent rule.

- **Purpose Limitation:** As a designated school official, Amira SbD uses all personally identifiable information (PII) from student education records for the sole and exclusive purpose of providing the student safety monitoring service, as explicitly defined in the contract with the school district. Student data is never used for targeted advertising, marketing, profile building, or any other commercial purpose unrelated to the provision of the educational service.
- **Direct Control:** The school district retains direct control over its student data at all times. The platform operates as a service provider acting on the school's behalf. The district has the right to review, amend, and request the deletion of its data in accordance with its own policies and FERPA regulations.
- **Prohibition on Re-disclosure:** Amira SbD is contractually and legally prohibited from re-disclosing any PII from education records to any other third party without the express, prior written consent of the school district, except as required by law.



Children's Online Privacy Protection Act (COPPA)

COPPA imposes specific obligations on the operators of online services that collect personal information from children under the age of 13. Amira SbD fully complies with these obligations.

- **School-Based Consent:** In the educational context, COPPA permits schools to provide consent on behalf of parents for the collection of student personal information, provided the service is used for a school-authorized educational purpose and for no other commercial purpose. Amira SbD operates exclusively under this provision.
- **Notice to Schools:** Amira provides each partner school district with a clear, comprehensive notice of its data collection, use, and disclosure practices. This notice enables the school to inform parents as part of its own technology use policies.
- **Data Retention Limitations:** In accordance with COPPA's requirements, personal information collected from children is not retained for longer than is reasonably necessary to fulfill the educational purpose for which it was collected. Specific data retention schedules are established in the contract with each school district to ensure timely and secure data destruction.

Children's Internet Protection Act (CIPA)

CIPA primarily requires schools and libraries that receive E-Rate discounts to implement technology protection measures (i.e., content filters) to block obscene or harmful content. While Amira SbD is not a content filter, it serves as a critical and complementary component of a comprehensive internet safety strategy.

Content filters are effective at blocking access to known inappropriate websites but are often unable to detect harmful content generated by students themselves within approved applications (e.g., cyberbullying in a school-managed document, expressions of self-harm in an email). Amira SbD addresses this gap by monitoring student-generated content for signs of distress or danger. This helps schools fulfill their broader CIPA obligation to monitor the online activities of minors and provides teachable moments for educating students on appropriate online behavior.

Compliance with State Laws

In addition to federal statutes, Amira SbD is committed to full compliance with the legal and regulatory framework of the State of Indiana. The platform is designed to be a responsible partner that respects the specific requirements and priorities of Indiana's educational system. The legal framework in most states for student data privacy relies heavily on the robust standards set by federal law, primarily FERPA. Amira SbD has adopted a proactive stance.

The platform is specifically configured to address state statutes related to student safety and technology:

- **Bullying Definition:** The NLP models are trained to recognize and flag language that meets Indiana's statutory definition of bullying, which includes "overt, unwanted, repeated acts or gestures, including verbal or written communications or images transmitted in any manner (including digitally or electronically)" as defined in IC 20-33-8-0.2.
- **District Cybersecurity Standards:** The platform acknowledges that under IC 20-25.7-4-6, a school corporation may require its technology partners to comply with specific networking and cybersecurity standards. The Amira SbD architecture is flexible and can be configured to meet the unique technical and security requirements of any Indiana school district.

Alignment With State Cybersecurity Priorities

Amira SbD recognizes the Indiana Department of Education's increasing focus on cybersecurity and its partnership with national organizations like the Consortium for School Networking (CoSN) to promote best practices for data protection in schools. The platform's robust security architecture, principled data handling protocols, and adherence to national security standards are directly aligned with the goals of initiatives like CoSN's Trusted Learning Environment (TLE) Seal Program. By providing a secure, transparent, and compliant service, Amira SbD supports Indiana schools in their efforts to build and maintain a trusted digital ecosystem for their students and staff.

Auditability and Record Keeping

Transparency and accountability are essential for building and maintaining trust with educational partners and parents. The Amira SbD platform is designed with comprehensive auditability at its core, ensuring that a secure and verifiable record of all actions is maintained. This capability is critical for internal oversight, incident investigation, and demonstrating regulatory compliance.

Immutable, Comprehensive Audit Trails

Every significant action performed within the Amira SbD platform is captured in a secure, tamper-resistant audit log. This includes actions taken by authorized school personnel who access the system, as well as actions taken by credentialed Amira SbD system administrators performing maintenance or support functions.

The audit trails are designed to ensure accountability and non-repudiation, meaning that an individual cannot deny having performed an action that was recorded.⁴⁰ Each log entry includes detailed information, providing a complete and chronological record of events that can be used for forensic analysis in the event of a security incident or for routine compliance reviews. The integrity of these logs is protected through strong encryption, secure storage, and strict access controls to prevent any unauthorized modification or deletion.

Secure Access, Retention, and Reporting

Access to audit logs is governed by a strict, role-based access control (RBAC) model. Only a limited number of authorized personnel within a school district, as defined by the district itself, are granted permissions to view audit data. This principle of least privilege ensures that sensitive log information is protected from unauthorized access.

Log retention policies are not one-size-fits-all. The platform allows each school district to define its own data retention schedule for both student data and audit logs, ensuring compliance with local policies and state record-keeping requirements. At the end of the retention period, data is securely and permanently destroyed.

To facilitate oversight, the platform provides a secure administrative portal where designated district personnel can search, view, and export incident reports and audit logs. This on-demand reporting capability allows districts to easily respond to internal inquiries or requests from external regulatory bodies. The table below details the key data fields captured in every audit log entry, providing a tangible demonstration of the platform's commitment to transparency.

Table 1: Audit Log Data Fields

Field Name	Description	Example
Event ID	A unique identifier for each log entry.	a1b2c3d4-e5f6-7890-1234-567890abcdef
Timestamp	The precise date and time of the event in UTC.	2025-10-26T10:00:00.123Z
User ID / Principal	The identifier of the user or system process that initiated the action.	principal@school.k12.in.us or SystemAlertModule
DSource IP Address	The IP address from which the action was initiated.	203.0.113.25
Action Type	The category of the action (e.g., Login, View Alert, Escalate, Close Case).	VIEW_ALERT
Target Resource	The specific data or object that was acted upon.	AlertID: 98765 / StudentID: 112233
Outcome	The result of the action (e.g., Success, Failure, Denied).	AlertID: 98765 / StudentID: 112233
Details	A human-readable description of the event with relevant context.	AlertID: 98765 / StudentID: 112233

Summary

Amira SbD offers a powerful, proactive tool to assist SEAs and LEAs in their fundamental mission to protect the well-being of every student. The platform is engineered to deliver timely and accurate alerts regarding students at potential risk of self-harm or violence, enabling educators to intervene effectively and provide necessary support.

This capability is delivered upon an unwavering foundation of ethical design principles. By embedding internationally recognized frameworks of Safety by Design and Privacy by Design into its core architecture, Amira SbD ensures that its safety mission does not come at the expense of student privacy. The platform's secure architecture, advanced contextual NLP engine, and robust notification systems are all designed to be precise, reliable, and respectful of the educational environment.

Amira has demonstrated its full and rigorous compliance with all relevant federal laws, including FERPA, COPPA, and CIPA, and its alignment with the SEA's specific legal codes and cybersecurity priorities. This commitment to compliance is reinforced by a system of complete transparency, providing school districts with comprehensive audit trails and administrative control over their data.

Works Cited

- School Safety | EdTech Magazine, accessed September 11, 2025, <https://edtechmagazine.com/k12/school-safety>
- Whitepapers – Raptor Technologies, accessed September 11, 2025, <https://raptortech.com/resources/whitepapers/>
- Public Schools, Private Eyes: How EdTech Monitoring Is Reshaping Public Schools – New America, accessed September 11, 2025, <https://www.newamerica.org/education-policy/edcentral/how-edtech-monitoring-is-reshaping-public-schools/>
- Student Privacy at Risk? EdTech Surveillance in Focus – ListEdTech, accessed September 11, 2025, <https://listedtech.com/blog/student-privacy-at-risk-edtech-surveillance-in-focus/>
- New ACLU Report Shines Light on Shadowy EdTech Surveillance Industry and the Dangerous Consequences of Surveillance in Schools | American Civil Liberties Union, accessed September 11, 2025, <https://www.aclu.org/press-releases/new-aclu-report-shines-light-on-shadowy-edtech-surveillance-industry-and-the-dangerous-consequences-of-surveillance-in-schools>
- Safety by Design | eSafety Commissioner, accessed September 11, 2025, <https://www.esafety.gov.au/industry/safety-by-design>
- Safety by Design: A responsible AI framework – Safer by Thorn, accessed September 11, 2025, <https://safer.io/resources/safety-by-design-a-responsible-ai-framework/>
- SbD: What It Is & Why It Matters, accessed September 11, 2025, <https://www.tspa.org/curriculum/ts-curriculum/safety-by-design/sbd-what-it-is-why-it-matters/>
- cesprivacy.org, accessed September 11, 2025, <https://cesprivacy.org/privacy-bydesign#:~:text=Privacy%20by%20Design%20mandates%20security,through%20to%20its%20secure%20disposal.&text=Privacy%20policies%20and%20operations%20must,and%20subject%20to%20external%20Verification.>

- Privacy by design – Wikipedia, accessed September 11, 2025, https://en.wikipedia.org/wiki/Privacy_by_design
- Privacy by Design, accessed September 11, 2025, <https://cesprivacy.org/privacy-by-design>
- Children's Code – Wikipedia, accessed September 11, 2025, https://en.wikipedia.org/wiki/Children%27s_Code
- UK Age Appropriate Design Code – 5rights, accessed September 11, 2025, <https://5rightsfoundation.com/resource/setting-new-standards-for-childrens-data-privacy-the-childrens-code/>
- FERPA 101 for EdTech Companies – iKeepSafe, accessed September 11, 2025, <https://ikeepsafe.org/content/uploads/2017/01/FERPA-101-for-EdTech-iKeepSafe.pdf>
- Responsibilities of Third-Party Service Providers under FERPA – Protecting Student Privacy – U.S. Department of Education, accessed September 11, 2025, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf
- Education Security Solutions – Check Point Software, accessed September 11, 2025, <https://www.checkpoint.com/industry/education/>
- Audit Trails in Cloud Governance for Compliance & Security, accessed September 11, 2025, <https://www.xcelligen.com/audit-trails-and-reporting-in-cloud-governance-through-detailed-logs/>
- NLP for Social Media Threat Detection: Guide – Cimphony.ai, accessed September 11, 2025, <https://www.cimphony.ai/insights/nlp-for-social-media-threat-detection-guide>
- Detection of Expressions of Violence Targeting Health Workers with Natural Language Processing Techniques – MDPI, accessed September 11, 2025, <https://www.mdpi.com/2076-3417/15/4/1715>
- Application of Natural Language Processing (NLP) in Detecting and Preventing Suicide Ideation: A Systematic Review – PMC – National Institutes of Health (NIH) |, accessed September 11, 2025, <https://pmc.ncbi.nlm.nih.gov/articles/PMC9859480/>

- Digital Threat Detection Software for Schools | Navigate360, accessed September 11, 2025, <https://navigate360.com/solutions/digital-threat-detection/>
- Monitor | Solutions | Linewize, accessed September 11, 2025, <https://www.linewize.com/solutions/monitor>
- School Emergency Alert System: Best Practices – Crises Control, accessed September 11, 2025, <https://www.crisis-control.com/blogs/school-emergency-alert-system/>
- FERPA-Compliant Contracts With Third-Party Risk Management – Venminder, accessed September 11, 2025, <https://www.venminder.com/blog/ferpa-compliant-contracts-third-party-risk-management>
- COPPA Guidance for Ed Tech Companies and Schools during the Coronavirus, accessed September 11, 2025, <https://www.ftc.gov/business-guidance/blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus>
- Does FERPA Impact Edtech Companies? – Edlink, accessed September 11, 2025, <https://ed.link/community/ferpa/>
- COPPA 101 for EdTech Companies – iKeepSafe, accessed September 11, 2025, <https://ikeepSAFE.org/content/uploads/2017/01/COPPA-101-for-EdTech-iKeepSafe.pdf>
- FTC Puts Edtech Companies on Notice of COPPA Compliance Investigations, accessed September 11, 2025, <https://www.loeb.com/en/insights/publications/2022/06/ftc-puts-edtech-companies-on-notice-of-coppa-compliance-investigations>
- E-Rate Central > Resources > Educational Information > CIPA, accessed September 11, 2025, <https://e-ratecentral.com/Resources/Educational-Information/CIPA>
- CIPA Compliance and Content Filtering – Lightspeed Systems, accessed September 11, 2025, <https://www.lightspeedsystems.com/solutions/security-compliance/cipa-compliance/>
- CIPA Compliance in Google Workspace for Education – GAT Labs, accessed September 11, 2025, <https://gatlabs.com/education/cipa-compliance/>

- Student Privacy, accessed September 11, 2025, <https://privacy.iu.edu/student/index.html>
- DOE: The Family Educational Rights and Privacy Act (FERPA), accessed September 11, 2025, <https://www.in.gov/doe/it/ferpa/>
- Indiana Privacy of School Records Laws – FindLaw, accessed September 11, 2025, <https://www.findlaw.com/state/indiana-law/indiana-privacy-of-school-records-laws.html>
- Bullying | Springs Valley Community Schools, accessed September 11, 2025, <https://www.svalley.k12.in.us/page/bullying>
- Indiana Code Title 20. Education § 20-25.7-4-6 | FindLaw, accessed September 11, 2025, <https://codes.findlaw.com/in/title-20-education/in-code-sect-20-25-7-4-6/>
- Indiana schools ramp up cybersecurity to safeguard student data – WFYI, accessed September 11, 2025, <https://www.wfyi.org/news/articles/indiana-cybersecurity-protect-student-data-consortium-school-networking>
- CoSN TLE Partnership Boosts Student Data Privacy in Indiana – GovTech, accessed September 11, 2025, <https://www.govtech.com/education/k-12/cosn-tle-partnership-boosts-student-data-privacy-in-indiana>
- Audit Log Best Practices for Security & Compliance | Fortra's Digital Guardian, accessed September 11, 2025, <https://www.digitalguardian.com/blog/audit-log-best-practices-security-compliance>
- Understanding Audit Trails – Uses and Best Practices | Ping Identity, accessed September 11, 2025, <https://www.pingidentity.com/en/resources/blog/post/audit-trail.html>
- Best practices for Cloud Audit Logs, accessed September 11, 2025, <https://cloud.google.com/logging/docs/audit/best-practices>
- Cloud Audit Logs overview – Google Cloud, accessed September 11, 2025, <https://cloud.google.com/logging/docs/audit>
- Audit Log Best Practices For Information Security – ZenGRC, accessed September 11, 2025, <https://www.zengrc.com/blog/audit-log-best-practices-for-information-security/>