Caderno: Mission and Vision Document

Table of Contents

Mission

Caderno is a privacy-first, decentralized journaling platform dedicated to safeguarding personal truths and empowering those who speak truth to power. Our mission is to provide **journalists, whistleblowers, survivors, and activists** with a secure digital space to document their experiences and insights without fear of censorship or surveillance. Users can record daily reflections or sensitive witness testimony in encrypted “journal pantries” stored on a decentralized cloud that **they** control. A core feature of Caderno is an optional safety mechanism (a form of *dead man’s switch*): users may set a timed **alarm** that, if triggered, automatically compiles and delivers their journal entries to pre-selected email addresses or phone numbers. This ensures that crucial information will be shared with trusted contacts in case the user is unable to do so themselves – a powerful safeguard **protecting users from those who might wish to silence or harm them**. By combining strong cryptographic protection with a federated (self-hostable) infrastructure, Caderno’s mission is to **put control back into the hands of the people**, enabling them to document truth and **preserve evidence with confidence and integrity**.

Vision

Our vision is a world where **personal narratives and critical truths are preserved securely, transparently, and resiliently** – beyond the reach of any single authority or adversary. We envision Caderno as more than just a journaling app: it is an **ethical digital sanctuary** that fosters transparency and **resilience** in the face of oppression or adversity. In this future, **empowered individuals speak truth to power** and hold the powerful accountable without fear, using technology that guarantees their voices cannot be erased. Caderno aims to set a new standard for journaling and personal documentation by normalizing **end-to-end encryption, decentralization, and user autonomy** as default expectations. By **federating** the platform, we see a rich ecosystem of user-operated servers around the world, collectively forming a network that is highly available and censorship-resistant. Ultimately, our vision is to **give power back to the people**: each user owns their data, controls their narrative, and can trust that their private thoughts or critical evidence remain secure yet ready to galvanize change when needed.

Ethos

Caderno's ethos is grounded in the principles of **transparency, resilience, and empowerment**, guided by a commitment to **privacy, security, and social accountability**. Our core values include:

- **Transparency:** We believe in openness in both technology and governance. Caderno is fully open-source, allowing anyone to inspect or contribute to the code. This transparency fosters trust and accountability – there are no hidden backdoors or secrets in how Caderno operates. *(In line with this principle, the source code is publicly available for scrutiny, affirming our commitment to trustworthiness[1].)* We also maintain clear communication with our community about our practices and updates, ensuring users are never in the dark.

- **Privacy: Privacy is a fundamental human right** and the foundation of our platform. Caderno is built from the ground up to protect user privacy, using end-to-end encryption for journal entries by default. Only the user (and whomever they explicitly share with) can read their entries – not us as developers, not any hosting provider, nor any third party. We **do not collect or monetize personal data**. In contrast to conventional note-taking apps that may have access to user content (for example, Google Keep lacks advanced safeguards like end-to-end encryption and even operates on an advertising-based model[2]), Caderno never exploits or analyzes the user's private writings for profit. Users retain full ownership and control of their data.

- **Security & Resilience:** We recognize that our users, especially **journalists and activists, face sophisticated threats** – from hackers and spyware to coercive forces. Caderno's design prioritizes robust cybersecurity measures to defend against these threats. All data is secured with modern cryptography (using strong encryption algorithms and best practices) both **in transit and at rest**. Because Caderno is **decentralized and federated**, there is no single point of failure: no central server that a malicious actor or censor can take down to compromise the network. This distributed architecture inherently provides **resilience against outages and censorship**, ensuring that even under hostile conditions, users can safely record and access their information[3]. Our ethos of security also means **constant vigilance**: we encourage third-party security audits and community reporting of vulnerabilities, and we respond transparently to any security issues. *We recall real-world cases where activists' devices and online platforms were infiltrated by adversaries (for example, spyware like NSO Group's Pegasus was used to surveil thousands of targets including journalists[4]); such incidents drive our relentless focus on hardening Caderno against intrusion.* In sum, our ethos is to **protect and preserve** – protecting user data from prying eyes and preserving their voice even in volatile circumstances.

- **Empowerment & Advocacy:** Caderno is not just a tool, but a means of empowerment. We stand for **user autonomy and freedom of expression**. By

giving users the ability to **self-host** their journals on servers they control, we eliminate dependency on big corporations or governments – **power is returned to the people**. Users can operate in whatever jurisdiction or environment they feel safest, or join a community-run server aligned with their principles. This federated model encourages a grassroots approach to information ownership. We see Caderno as part of a larger movement to **democratize technology and uphold digital rights**. In practice, this means we design features specifically to support those who risk much to tell the truth: for example, the aforementioned journal alarm feature embodies **"speaking truth to power"** by acting as a form of insurance – even if someone tries to silence a whistleblower, their story will still come out. Our ethos compels us to support these courageous users: **Caderno stands with the whistleblower, the survivor, and the activist**. We are inspired by the principle that encryption and secure communication enable advocacy groups and individuals to hold the powerful accountable[5]. By using Caderno, users can "write fearlessly" knowing the platform is on their side, prioritizing their safety and mission.

- **Accountability & Integrity:** We strive to create a culture of accountability – both for ourselves and as a tool for users to hold others accountable. Internally, we hold ourselves to high ethical standards in developing this app (e.g. no dark patterns, no compromising on security for profit). Externally, Caderno's very purpose is to help **document truth with integrity**, creating immutable records (through cryptographic timestamping or future features like content versioning) that can serve as evidence. We treat a user's journal, especially if it contains witness testimony or evidence of wrongdoing, as sacrosanct. With the user's consent, Caderno can ensure these records are **available to trusted parties or the public** (in redacted or summary form) in case of emergency – shining a light on truths that might otherwise be buried. This fosters a form of *social accountability*, where bad actors know that harming an Caderno user could trigger the exposure of the very information they wish to suppress. In this way, the platform aligns with the ethos of *justice and empowerment*, reinforcing that **the truth will find a way out**.

In summary, Caderno's ethos is defined by a deep respect for user rights and a proactive stance in **defending those who defy silence**. We champion **transparency** in how we operate, **resilience** in technology and community, and **empowerment** of every individual's voice. These principles aren't just words on paper for us – they are the guiding light in every decision, feature, and policy associated with Caderno.

Privacy

Privacy is paramount in Caderno's design and operation. We recognize that in many cases, a journal entry isn't just a private thought – it could be sensitive information that, if exposed, might endanger the writer or others. Therefore, Caderno employs rigorous privacy protections to ensure users can write freely and **confidentially**.

End-to-End Encryption: All journal entries can be end-to-end encrypted (E2EE) by the client before being stored or sent anywhere. This means entries are **encoded in such a way that only the author (and their intended recipients, if any) can decrypt and read them**[6]. Even if a server hosting the data is compromised or someone intercepts the data, the content remains unintelligible without the decryption keys. Caderno's encryption model covers data at rest and in transit – journals are encrypted on the user's device and stay encrypted on the server, with secure protocols used for any data transfer. *There are absolutely no "back doors" or special access keys.* Not even Caderno's developers or a server administrator can read the encrypted entries, which underscores our zero-knowledge approach to user data. This level of security is non-negotiable: as advocacy groups and privacy experts note, **end-to-end encryption is the best assurance that personal data and communications are shielded from prying eyes**[7].

Federated, Decentralized Storage: Privacy is also enhanced by Caderno's federated architecture. Users can choose to host their journals on their own server or pick a trusted host (for example, a non-profit organization, a community collective, or a friend) rather than a monolithic corporate server. Because any user can spin up their own Caderno server, it **eliminates centralized data silos** that are attractive targets for mass surveillance or hacks. Each server operates independently, sharing no more data with the network than necessary. *If you run your own server, your data lives on hardware you control; if you use someone else's server, you've at least chosen one that aligns with your privacy expectations.* In either case, federation prevents any single entity from having access to all user data. This decentralization is a stark contrast to mainstream cloud note services where one company stores millions of users' notes in one place. Our approach drastically reduces the risk of large-scale privacy breaches.

No Tracking or Data Monetization: Caderno does not and will not engage in any form of tracking beyond what is absolutely necessary for security (for instance, basic logging to detect abuse, which is done transparently and, where possible, anonymized or pseudonymized). We do not use analytics that profile our users' behavior, and we certainly do not scan journal content for advertising or other monetization. Unlike some popular free journaling apps that rely on advertising or data mining (e.g., **Google Keep's revenue model is advertising-based, meaning user data can be leveraged for targeting[8]**), Caderno's open-source, user-centric model is **user-funded and community-driven**. Our commitment is that your data will only ever serve you, not us. We also provide an **offline-first** experience: users can create and read entries offline; sync is optional. This means you can keep your journal purely local (fully off the cloud) if you desire absolute isolation.

User Anonymity and Pseudonymity: To use Caderno, we minimize required personal information. Users may sign up with just a pseudonym/username and an email or phone *only if necessary* for features like the emergency alarm. Even then, such contact info is stored in encrypted form on the server. For those at risk, we encourage using secure, anonymous email accounts or dedicated phone numbers. Federated servers may have their own registration policies, but the official Caderno project provides guidance on privacy-friendly setup. Additionally, because federation allows communities of trust, users might join servers specifically catering to journalists or activists where privacy norms are strongest. Our aim is that **users should feel safe to express themselves without revealing their identity** unless they choose to.

Transparency and Control: Privacy is also about giving users control over their own information. Caderno provides intuitive settings for users to manage their data. This includes the ability to export all entries at any time (in an encrypted form or plaintext as the user chooses), to permanently delete entries (wiping them from the server), and to configure which contacts will receive their journal in an emergency. All such features are built to **empower the user's agency over their data**. We are transparent about how data flows through Caderno: for example, if a user enables the journal alarm feature, we explain how their entries will be compiled and encrypted for delivery, and that the app will periodically check a "heartbeat" to know when to send (with this check itself done in a privacy-preserving way). Users are always in the driver's seat – features are opt-in and customizable.

Differentiation from Mainstream Apps: Caderno's strict stance on privacy sets it apart from typical journaling or note-taking apps. For instance, Apple's new iOS Journal app emphasizes privacy and uses on-device processing, yet it remains a **closed ecosystem** tied to Apple's platform[9]. Apple's solution does offer end-to-end encryption for iCloud-stored entries[10], which we applaud; however, one must still *trust Apple's implementation and infrastructure*, and it's limited to Apple devices and services. In contrast, Caderno's open-source nature allows independent verification of its privacy claims, and its federated model ensures you're not locked into a single vendor or device family. Likewise, Google Keep (and similar cloud note apps) are designed for convenience over confidentiality; as mentioned, Google's employees or attackers with access to Google's servers **could theoretically read Keep notes** since they are not end-to-end encrypted[11]. Caderno rejects that trade-off – we choose privacy over Big Data convenience. Your Caderno journal remains **your eyes only** until you decide to share it.

In summary, privacy in Caderno is not just a feature – it's the default and the foundation. We leverage cutting-edge encryption and a decentralized architecture to ensure that **only you control access to your thoughts and experiences**. By doing so, Caderno creates a space where **honesty and vulnerability can thrive** without fear, and where even the most sensitive information (be it a personal reflection or evidence of corruption) is under **lock and key that only you hold**. Our motto could well be: *"Your story, your control"*, reflecting our unwavering commitment to user privacy.

Cybersecurity

Ensuring robust cybersecurity is crucial for an application that promises protection to high-risk users. Caderno approaches security with a **holistic, defense-in-depth strategy** to safeguard user data and the platform's integrity against threats. Our security philosophy can be summarized as *"trust no one, verify everything"* – not even us – which aligns with zero-trust principles and the idea that security should rely on mathematics and design, not on trusting people or companies[12].

Key aspects of Caderno's cybersecurity plan include:

- **State-of-the-Art Encryption:** As noted in the Privacy section, Caderno uses strong encryption standards (such as AES-256 and RSA/ECC or even post-quantum algorithms as they become practical) to protect data. We implement **end-to-end encryption (E2EE)** for journal content, which ensures that even if the data is stored on a server or in transit across a network, it's indecipherable without the user's private keys[13]. We apply modern cryptographic protocols (like TLS 1.3 for network connections) to prevent eavesdropping. Critical processes, such as the *journal alarm distribution*, are also encrypted. For example, if a user's compilation of entries is scheduled to be sent to contacts, that package is encrypted with the recipients' public keys ahead of time; thus, even if someone intercepts the package or the server is compromised, the content remains secure[14]. *By designing features with encryption at their core, we ensure that no sensitive data ever appears in plaintext on any intermediate system.* This approach has a clear benefit: a breach of an Caderno server would not leak readable journals – the attackers would only obtain ciphertext they cannot read.

- **Federated Security Model:** In a federated network, each server (or "instance") is administratively separate. This limits the blast radius of any single security incident. If one server has a vulnerability or gets breached, only the data on that server is at risk, not the entire user base. We provide guidelines and tools for server operators to secure their instances (such as recommended firewall settings, automatic updates, intrusion detection, and default configs that follow security best practices). Moreover, federation allows private instances: if a journalist wants absolute security, they might run Caderno on a closed server just for themselves, massively reducing exposure. Our network protocols between servers are minimal and authenticated, to reduce trust between instances – one compromised server cannot impersonate another or eavesdrop on private data exchanges. In essence, **decentralization is a security feature**: it avoids the peril of one central honeypot containing everyone's data and credentials. This also aids **censorship-resistance** – with servers in many jurisdictions, it's extremely hard for an attacker or authoritarian entity to block or shut down Caderno entirely[3]. Users can migrate between servers (with their data) if they lose confidence in a host's security, thanks to planned data portability features.

- **User Security Features:** Caderno incorporates features to help users protect themselves. For example, we offer **multi-factor authentication (2FA)** for account access on servers (e.g., TOTP or hardware key support) to mitigate the risk of stolen passwords. We encourage strong passphrases for encrypting journals, and the app can integrate with secure hardware enclaves or password managers for managing keys safely. The client applications can have an **app lock** (PIN or biometric) so that even if someone gains access to your device momentarily, they cannot open the Caderno app without authorization (similar to how secure messaging apps implement a lock). Additionally, there is an option to **mask or hide sensitive entries** on the screen (for instance, a "panic mode" that quickly conceals the app or certain notes) – useful in situations where a user is compelled to show their device. We also consider anti-tampering: the app will detect if its code has been modified (for example, by malware on a device) and warn the user or refuse to run if integrity is compromised. All these measures align with protecting users who might be under active threat.

- **Secure Development and Auditing:** The Caderno project follows secure software development life cycle practices. This means our code is reviewed for security issues, we leverage static analysis and dependency auditing tools to catch vulnerabilities, and we promptly patch any issues discovered. Being open-source, we invite independent security researchers to audit our code. We plan to undergo periodic **third-party security audits** for critical components (similar to how Standard Notes underwent third-party security auditing[2]) and will publish the results for full transparency. We also maintain a responsible disclosure program (or bug bounty program) to encourage and reward contributions from the security community. Importantly, because our ethos forbids secret backdoors, **any security weaknesses can be openly identified and fixed** – there is no obfuscation or denial. Users can inspect cryptographic routines to verify their soundness. By leaning on community expertise, Caderno's security can continuously improve, which is crucial as new threats emerge.

- **Protection Against Common Threats:** We harden Caderno against a range of known attack vectors. **Server Hardening:** Official Caderno releases come with security-hardened configurations (e.g., strict transport security, content security policy for web interfaces, rate limiting to prevent brute-force attacks, and sandboxing of processes). **Database Security:** User data on servers is encrypted at rest (layered on top of E2EE, so even server admins must take extra steps to access raw data). Keys used for server-side functions are stored securely, and we avoid storing any sensitive plaintext. **Network Security:** All inter-server communication is signed and encrypted, preventing man-in-the-middle attacks. **Client Security:** The client apps (mobile, desktop, web) are signed and verified to prevent tampering and will use secure APIs (for example, employing certificate pinning when connecting to a known server). We also guard against **supply chain attacks** by reproducible builds and package verification, so that users downloading the app can be confident it hasn't been maliciously

modified. **Privacy Threats:** We don't just secure against hackers, but also against unwarranted data requests. Since we don't hold plaintext data, even if we receive government subpoenas or requests, we cannot hand over journals in readable form – our system design itself is your privacy defense. We would also transparently report any such requests (warrant canaries, etc., in jurisdictions where applicable).

- **Emergency Response & Safety Mechanism:** Perhaps one of the most distinctive security aspects of Caderno is the **journal alarm (dead-man switch)** feature which intersects safety and cybersecurity. When a user enables this, their journal entries (or a subset) are packaged for later release. We treat this package with extreme care: it is **encrypted with the intended recipients' keys and possibly an additional layer of the user's own key**. The server or service that triggers the release does not need to know the content (and indeed cannot decrypt it). The timing mechanism (the "switch") is implemented securely – for example, the user might have to periodically enter a secret or proof-of-life token, and if they fail to do so by the set time, the system queues the release. This design ensures there's **no single point where an attacker could hack and prematurely obtain the info** (a known risk if dead man's switches aren't encrypted[15]). By requiring the attacker to also compromise the recipients or break strong encryption (both highly unlikely), Caderno's safety trigger **deters coercion and attacks**. It flips the script: if an adversary considers harming the user or seizing their device, they know that any such attempt could trigger the very outcome they fear – dissemination of the user's evidence. This acts as a powerful **preventative security measure** for the user. We cite real scenarios: *a whistleblower might set such a switch to release documents if they disappear, which only achieves its goal if implemented with robust encryption and authentication[14].* Caderno builds this scenario into a user-friendly feature, so users don't have to jury-rig their own solution.

- **Continuous Improvement:** Cybersecurity is not a one-time effort but an ongoing commitment. We will continuously monitor the landscape of threats (e.g., new spyware targeting activists, vulnerabilities in underlying software libraries, etc.). For instance, if a vulnerability in a cryptographic algorithm is discovered, Caderno will proactively update to stronger methods (our modular crypto design makes this feasible). We also plan regular updates and encourage users to keep their clients and servers updated by providing easy update mechanisms. Given our target user base may operate in dangerous environments, we also focus on **incident response**: if a user suspects their Caderno account or server is compromised, we provide clear steps to recover or migrate their data securely, revoke access, and communicate securely with them to resolve the issue. We also share cybersecurity knowledge with our community (educating users on how to secure their devices, use our tools safely, etc., since an app can only do so much if the endpoint device itself is compromised).

In conclusion, Caderno's cybersecurity measures are **comprehensive and tailored to defend high-risk users**. By combining strong encryption, a federated trust-minimized architecture, rigorous development practices, and innovative safety features, we strive to make Caderno a fortress for your personal writings and evidence. We understand the stakes – breaches or leaks are not just embarrassing, they could be life-threatening for some users. That reality drives us to leave no stone unturned in securing Caderno. Our pledge is that we will continue to fortify the app as technology and threats evolve, so that **users can journal with peace of mind**, focusing on their story and mission while we handle the shields and locks.

Monetization Plan

Caderno is envisioned as an open-source, decentralized application, which means traditional profit models (like selling user data or advertising) are off the table – by design, to uphold our privacy ethos. Nonetheless, to ensure the project's sustainability and growth, we have a thoughtful **monetization plan that aligns with our values**. Our goal is to **fund development and operations in ways that *enhance*, rather than compromise, user trust and empowerment.** Below are the key components of our monetization strategy:

- **Open-Source SaaS (Hosting Services):** We will offer an optional *managed hosting service* for Caderno journals – essentially a **hosted cloud version of Caderno** for users who do not want to run their own server. While anyone can self-host Caderno for free (the software is open-source), running a server requires some technical knowledge and effort. Our paid hosting will cater to users who value convenience: we'll run an Caderno server for them, handle updates, backups, and security maintenance, in exchange for a subscription fee. Importantly, even on our hosted service, user data remains end-to-end encrypted – we are charging for the service, not for access to their data. This model is often called *OpenSaaS* (open-source software offered as Software-as-a-Service) and has proven viable for many open source projects[16]. We will price it fairly, ensuring it's affordable while also balanced so that self-hosting remains an attractive free option for power users. The revenue from subscriptions will fund ongoing server costs and allow us to continuously improve Caderno. By bundling hosting with excellent customer support and perhaps extra conveniences (like one-click setup, custom domain, or increased storage), we provide value worth paying for without restricting the freedom of those who prefer to self-host.

- **Enterprise and Organizational Solutions:** We anticipate that certain organizations – for example, investigative journalism outlets, NGOs, or human rights organizations – might want to deploy Caderno for their teams. We can monetize by offering **enterprise support contracts or customized solutions** for these cases. This could involve helping set up a private federated network of Caderno servers for an organization, integrating Caderno with their existing IT infrastructure, or building custom features that they need. Organizations dealing with sensitive data might especially appreciate the combination of encryption and self-hosting. We could offer hosted enterprise instances with enhanced administrative tools, or a consultancy model where we assist their IT staff in deployment. In line with open-source norms, the core software remains the same for everyone, but enterprises would pay for **priority support, training, and custom development**. This approach lets us capture value from clients with resources, while the improvements can often be rolled back into the open-source project, benefiting all users. It's a model used by many open source companies (e.g., offering paid support is a mainstream way to earn money while keeping the software free[17]).

- **Donations and Sponsorships:** Given Caderno's mission-oriented nature (supporting free expression, privacy, etc.), we believe many users and institutions will **voluntarily support the project**. We will set up channels for donations – for instance, using platforms like **Open Collective**, which enable transparent funding of open-source projects[18]. Through Open Collective or similar, individuals who believe in Caderno's cause can contribute one-time or recurring donations. We will also pursue sponsorships and grants from organizations aligned with our values: think digital rights foundations, privacy advocacy groups, or even tech companies that support open-source privacy tools. Such sponsors could provide funding without dictating the project's direction (we will publicly disclose sponsorship to maintain transparency). We have inspiration from other projects in this vein (for example, SecureDrop, an open-source whistleblower submission system, is grant- and donation-funded by media organizations and nonprofits). With a clear mission of empowering voices and protecting truth, Caderno is well positioned to attract **philanthropic or community funding**. We may run fundraising campaigns highlighting how contributions directly help journalists and activists around the world. All funds raised through donations will be reinvested into development, security audits, and subsidizing services for users who cannot pay.

- **Premium Features or Add-Ons (Open-Core Model):** The base Caderno app will always be free and fully functional for private journaling. However, we may introduce **optional premium add-ons** for power users as a monetization lever. This might include advanced features that are not essential to the core mission but provide enhanced convenience or capabilities. Examples could be: AI-assisted journaling insights (if implemented in a privacy-preserving way), additional encryption key management options for organizations, secure cloud backup service beyond self-hosted options, or integration with other tools (say, an encrypted publishing workflow to selectively share journal entries as blog posts). These features could be offered under a modest subscription or one-time purchase. We will be very cautious here: any premium feature must not undermine privacy or create a walled garden; ideally it's more about **convenience and extended use-cases** rather than core security. We might adopt an *open-core* approach where the core remains fully open-source, while some peripheral tools or services are proprietary to paying customers. That said, we lean toward keeping as much as possible open-source; another approach is to have all features open, but paying users get early access to new features or priority in feature requests (this can overlap with the enterprise/custom model). We're exploring what premium offerings make sense that **do not fracture the user community or exclude those who can't pay**.

- **Community Marketplace (Long-term Idea):** As Caderno grows, there could be scope for a **marketplace or ecosystem** of related tools, templates, or plugins. For example, perhaps some developers create plugins for Caderno (such as unique cryptographic tools, or visualization dashboards for your journaling

patterns). We could allow a marketplace where third-party developers sell add-ons, and we take a small commission. This would stimulate an ecosystem and indirectly generate revenue. Another angle: if some users want physical products (like a hardware secure journal device, or merchandise supporting the cause), that could be a minor revenue stream too. These are tentative ideas for the future; the immediate focus is on the service and support models.

- **No Advertisements or Data Sales – Ever:** It's important to state what *we will not do*. We will **never monetize Caderno through ads, user data analytics, or selling user information**. Those methods would violate our core principles of privacy and trust. We won't impose paywalls that hinder basic access to the tool for those in need. Monetization is approached as a way to sustain the project and enhance it, not to exploit the user base. Our financial viability will come from providing genuine value (like reliable hosting or expert support) that users or sponsors are willing to pay for, rather than from turning users into the product. We understand this may cap potential profit, but Caderno is a mission-driven project first and foremost. We are confident that by building a strong reputation and user community, the project can attract sufficient financial support through the above ethical avenues.

- **Transparency in Finance:** In line with our ethos of transparency, we will maintain open accounting of how the project is funded. If we raise money through Open Collective or donations, those ledgers are public. If we earn revenue from hosting or enterprise deals, we intend to share high-level numbers with the community in annual reports. Users will know that their subscription dollars or donations are going toward things like paying developers, running servers, security audits, community outreach, etc. This transparency helps build trust that monetization isn't making someone rich at the expense of the mission; instead, it's fueling the mission. We also plan to **reinvest profits** into providing free or discounted services for at-risk user groups (for example, setting up free hosting for a coalition of independent journalists in repressive regions, subsidized by paying customers elsewhere).

To summarize the monetization plan: **Caderno will sustain itself through a combination of premium services, support, and community goodwill – all aligned with our open-source, user-first philosophy.** By offering optional paid conveniences (like managed hosting and enterprise support) and encouraging community funding, we can keep the project healthy and evolving. This approach has precedent in successful open-source projects and ensures that **our incentives remain aligned with our users**. We succeed only by making a tool people find valuable enough to support – not by betraying their trust.

In the long run, we believe this model will not only monetize Caderno effectively but also strengthen its community. Users who financially support Caderno become stakeholders in its success, creating a virtuous cycle: their funding improves the app, which in turn better serves them and attracts more users. With prudent management and a focus on

our core values, Caderno can **achieve financial sustainability without ever compromising the privacy, security, or empowerment of its users**. This is how we intend to build a lasting platform that genuinely serves the public good while standing on solid economic ground.

Conclusion: Caderno's mission, vision, ethos, and strategies collectively paint the picture of a unique journaling platform — one that is **open, secure, and built for those who need it most**. By adhering to our principles and smartly navigating monetization, we aim to prove that technology can be both socially responsible and sustainable. Caderno will always prioritize the **people** who use it and the **truths** they bravely record. Together with our community, we are building more than an app; we are building a movement of **privacy, transparency, resilience, and empowerment** for all who have a story to tell and a truth to safeguard.

Sources:

1. Standard Notes Team – *Security and Privacy Comparison of Google Keep vs Standard Notes* (Standard Notes Blog)[2][19]
2. Apple Newsroom – *Apple's Journal App Privacy Features*[10]
3. Cybernews – *Apple Journal app limitations*[9]
4. Internet Society – *Encryption as a Tool for Advocacy and Human Rights*[5][4]
5. Sasha Shilina (Medium) – *Advantages of Decentralized Networks (Privacy, Censorship Resistance)*[3]
6. Cipherwill Blog – *The Need for E2EE in Dead Man's Switch for Whistleblowers*[14]
7. Scaleway Blog – *Monetization Models for Open-Source Projects*[16][17]
8. Open Collective Documentation – *Funding Open-Source via Open Collective (Donations)*[18]
9. Standard Notes – *Google Keep's Lack of E2EE and Advertising Model*[20]
10. Standard Notes – *Public Source Code and Transparency as Trust Builders*[1]
11. Reddit (r/privacy) – *Google Keep Employee Access to Notes (no end-to-end encryption)*[11]

[1] [2] [8] [11] [19] [20] What makes Standard Notes a great Google Keep alternative End-To-End Encrypted Notes App

https://standardnotes.com/compare/google-keep-alternative

[3] The future of social networking: Decentralization for user empowerment, privacy, and freedom from censorship | by Sasha Shilina | Medium

https://medium.com/@sshshln/the-future-of-social-networking-decentralization-for-user-empowerment-privacy-and-freedom-from-a0a8f74790cb

[4] [5] Factsheet: How Encryption Can Protect Advocacy Groups and Social Change Movements - Internet Society

https://www.internetsociety.org/resources/doc/2021/factsheet-how-encryption-can-protect-advocacy-groups-and-social-change-movements/

[6] [12] [13] [14] [15] Why Dead Man’s Switch Need End-to-End Encryption

https://www.cipherwill.com/blog/why-dead-mans-switch-need-end-to-end-encryption-1fb6d63626188008a410ea6fea4bfaae

[7] The Vital Role of End-to-End Encryption | ACLU

https://www.aclu.org/news/privacy-technology/the-vital-role-of-end-to-end-encryption

[9] Apple's Journal app: a breakthrough in digital diary-keeping or a privacy concern? | Cybernews

https://cybernews.com/editorial/apples-journal-app-privacy/

[10] Apple launches Journal app, a new app for reflecting on everyday moments - Apple

https://www.apple.com/newsroom/2023/12/apple-launches-journal-app-a-new-app-for-reflecting-on-everyday-moments/

[16] [17] [18] How to monetize your open source project (and pay your developers) | Scaleway Blog

https://www.scaleway.com/en/blog/how-to-monetize-your-open-source-project/