PROJECT 4

REPORT DUE: OCT, 14

Company Summary: Creating a secure cyber space with the help of AI and the most advanced cryptographic algorithms.

1. **Ethical Business Plan (1500 words):**
    a. ClearAI Security
    b. **[1.B. Long-Term Vision Statement -** Clear AI Security plans on being the forefront of leading Cryptographic AI security, sprawling with new algorithms and methods of securing the digital world, using quantum computing and AI to lead us into the future, we envision the usage of AI as a tool and for innovation and a safeguard against cyber attacks, Our mission is to anticipate, neutralize and annihilate any treat presented, with the understanding of AI, we will use its own patterns to identify the malwares that may be created from the same source(AI), with this keeping systems secure, ethical and resilient, creating a safety space where we prioritize the security of our users, by encryption of their information even from our resources and just having access to them by different AI keys will be a factor that can avoid any leak of information even in between the organization

        i. **[1.B.1 Goals**] Building cutting edge cybersecurity software driven by AI and quantum computing technologies is the main objective of ClearAI Security, which aims to usher society into a safer and more secure digital future. Our goal is to develop systems that can withstand even the most advanced threats brought about by AI while maintaining the integrity, openness, and resistance to abuse of our solutions. Our goal is to protect people, companies, and governments by creating scalable platforms without compromising their basic rights to privacy and self-determination. Ensuring that our technologies cannot be monopolized, exploited, or repurposed by corporations or governments to restrict freedom, is the main key point that we are aiming for. Rather, by returning power to the user, ClearAI Security aims to promote accessibility, equity, and trust in all spheres of society. As part of this effort, we will also try to end the growing prevalence of misleading digital policies—those unspoken contracts and deceptive tactics that let businesses take advantage of customer data with little to no compensation. We're determined to replace those methods with open, user-centered security measures that improve daily life and boost digital trust.

        ii. **[1.B.2 Idea Origination**] A passion project that I plan on making into fruition once I have the ability to do so. A passion for defending digital

liberties in a world increasingly powered by AI gave rise to the concept for ClearAI Security. The idea of pursuing the path of cybersecurity and the evolution of AI would be a good combination, since these are the expected areas to have growth for the following years. Knowing that it will evolve in the following years also means that it can be used to harm others, why not creating a defense over it, to avoid the usage of AI into this labors that are not beneficial for the communities, having AI to battle AI is the key point since it can understand itself and the way how it operates based on the probabilities created by the patterns that they follow at the moment of executing their actions.

iii. **[1.B.3 Purpose/Values/Mission]** ClearAI Security's goal is to make sure that no organization, government, or business can illegally access protected devices or take advantage of personal data. We are dedicated to fostering an atmosphere of total and independent privacy in everyday living where people can rest assured that their online personas are safe from infringement. Because our systems are specifically built to withstand automated attacks, such as botnets and brute force attempts, malicious actors cannot compromise private information. Transparency, trust, and moral responsibility are the cornerstones of our values. We promise never to use our clients' information for manipulation or financial gain because we think protecting data should never come at the expense of doing so. Our goal is to protect data without any covert agendas, intrusive tracking, or dishonest tactics. By doing this, ClearAI Security hopes to transcend beyond just a business and become a representation of empowerment and resiliency into this new digital era which everything is unseen, protecting people from technological abuse, exploitation, and unlawful surveillance.

iv. **[1.B.4 Key Questions:** For instance, how can the startup have an impact? What engages our passions?] What can be changed to ensure that government entities can have no control of our freedoms of life and liberty? Can we find a solution in which all aspects of data transfer and stored memory is impenetrable from bad actors or unwanted intruders, protecting against common traffic hijacks and any other methods of government access to locked data? With the development of quantum computers and AI, are there new algorithms that can be perfected with the help of AI while using quantum computers? In essence, a means of encrypting something and it is unbreakable b/c of AI and QC during the first time implemented. Can we have AI protect and oversight

all data at every moment of the day? How can we analyze AI entities and botnets that have human patterns?

v.

c. Testing: write here if adding input. **[1.C. Strategy with Ethical Impacts AND Ethical Safeguards**: for the next 3 to 5 years you will create a list of OKRs w/ metrics, Experiments, Ethical impacts/issues and Ethical Safeguards. **You should have a minimum of 3 OKRs** . The documentation for EACH OKR is 500 words minimum (total for 3 OKRs is 1500 words minimum)]

OKR1: Establish Rapid Threat-Response AI System

Objective:

Build a self-learning AI threat-detection network that responds to new cyberattacks in real-time without human delay.

*Detect and neutralize 95% of attempted intrusions within 3 seconds of detection.
*Reduce manual analyst interventions by 70%.
*Deploy autonomous monitoring nodes in 5 high-risk client networks by Q3 2026.

OKR2:

1.C.1.1 OKR 1 Objective and Key Result

ClearAI Security will incorporate encryption, transparent reporting, and AI-powered monitoring to ensure complete data privacy and compliance with global regulations, so we can create a better community and be trusted aroudn the world. This OKR focuses on protecting private user data from unauthorized access while upholding global privacy standards such as the CCPA and GDPR. Every client, be they a small business, enterprise organization, or individual user, should be able to trust the initiative to handle, protect, and never sell their digital data.

1.C.1.2 OKR 1 Metric(s) with Experiment(s)

For us to measure the success of this OKR, ClearAI Security will track three main metrics which will be the base of our systems and organization: data breach frequency, employee training completion, and privacy audit performance.

The Incident-Free Rate: no data breaches within a 12-month period

The Employee Ethics Training Completion Rate: 100% staff compliance

The Audit Performance Score: fewer than two minor findings per independent audit

The first experiment will focus on the Incident-Free Rate, this tris probing statistically how secure we are in order for us to improve in different areas. The

second experiment will evaluate internal accountability through the Ethics Training Completion Rate, with this securing our people and customers in order to create a more safe environment inside the organization. The final experiment will assess compliance through Independent Privacy Audits, with this managing information and checking independently with customers about their agreement with our policies.

1.C.1.3 OKR 1 Ethical Impact(s)/Issue(s)

Ensuring Data Privacy and Regulatory Compliance: Over-collection of data, bundled or ambiguous consent, excessive log retention for AI improvement, or insufficient vendor controls can all lead to ethical risks even with high security. These issues could violate user privacy and autonomy, hurt ClearAI's finances and reputation, and aggravate regulators and auditors.

Expected Ethical Impact Risk Table

Stakeholder	Financial Risk	Privacy Risk	Conflicting Interest Risk	Violation of Rights Risk
Customer / End User	Low	High	Mid	High
Company (ClearAI)	High	Mid	Mid	Mid
Government / Regulators	Low	Low	Mid	Low
Third-Party Auditors	Mid	Mid	Mid	Low

1.C.1.4 OKR 1 Ethical Safeguards

Every new feature must undergo a Data Protection Impact Assessment (DPIA) both during design and again prior to launch as part of the privacy-by-design with a DPIA gate. 100% DPIA completion across releases, zero high/critical risks at launch, an average time-to-mitigate of less than 30 days, and consistently rising independent-audit pass rates will be the metrics by which we measure efficacy.

ClearAI will formalize a vendor program. Prior to onboarding, vendors sign data-processing agreements and fill out a security/privacy questionnaire accompanied by supporting documentation. 100% of vendor reviews finished before access, zero

significant vendor caused incidents, and less than 30 days of remediation for findings are indicators of effectiveness.

OKR3

CHECK OKR AT BOTTOM OF THIS SECTION ON PROF. WEBPAGE!

2. **Cultural Policy** (minimum 300 words) DON'T CHANGE SECTION NAMES! E.g., Core Values, etc.

a. [**2.A. Core Values]** We want to provide as much freedom to our clients as possible, to never have our conversations, data, or information exploited. To ensure that our clients can be protected from an unjust government/ corporation that intends to use our passions and intentions towards their needs. As all humans deserve to live, is to live without threat of their lives and freedoms. So that no matter what enemy tries to steal, exploit, or expose your intellectual properties, they are safe when using our AI, Quantum Computed, Cryptographic algorithms to keep this information away from being used to regulate us and keep creating this chain which doesn't allow people to be free and express their real needs.PURE UNADULTERATED PRIVACY, ENCRYPTION, AND CYBER SECURITY.

b. ***[2.B. Motivation]*** We are completely intrigued by cybersecurity, this is where it all started. We then fell in love or engulfed ourselves into understanding the secrecy of translating languages into arbitrary concepts to fool those that wish to harm you. With this goal, our vision was to develop knowledge and mix powerful concepts with the speed of AI at the moment of generating our ideas. We love the idea of how important cryptography is but it's not openly spoken about. The idea of how the power is given to every person in the world motivates us to continue expanding with new inventions into the project, knowing that we all have the free will but the fears of getting dominated by big entities or having our information filtered is what retains us humans to explore and continue innovating. I fear the government and private entities under its control. Corporations are out to engage in exploiting the national populace, foreign and domestic. Fear that governments use the excuse of national security to limit and attack their citizens to enslave them to their commands. Besides all this, they're using our information free and against us just to keep a regulation that benefits the hierarchy the most.

c. [**2.C. Summary**: summary in 6 words or less the company's culture]

1. Privacy
2. Security
3. Ethics

4. Innovation
5. Freedom
6. Resilience

3. **Ethical Policies** (300 Words)

a. **[3.A. Core Items -** Enumerate the core items in your ethics policy and give details of each policy item and its meaning.]

1. **Privacy as a Human Right**: Personal privacy will not be compromised by ClearAI Security. Our AI and encryption solutions are all made to prevent unauthorized access to private information by people, businesses, and governments. This pledge guarantees each user's autonomy and dignity.

2. **Accountability and Transparency**: We will allow independent audits of our algorithms, especially those pertaining to AI based threat detection. To make sure our tools are not abused for unethical or surveillance-related purposes, we will permit external oversight and publish transparency reports.

3. **Ethical Innovation**: We pledge to never develop offensive cyberweapons using AI and quantum computing, only for defensive applications. Our goal is to ensure that technological advancements responsibly serve society by emphasizing resilience rather than escalation.

4. **Fair Access and Non-Exploitation**: ClearAI Security will not permit businesses or governments to monopolize our systems. In order to stop powerful actors from taking advantage of citizens in the name of "national security," we want to keep our solutions accessible and scalable.

b. [3.B. Board - List 3 real people (maybe tech leaders) that you want on your board, a brief bio, AND why you chose them for the board. (*write in full paragraphs, not bullets).* ALL members should have some experience in the tech sector of your company (e.g., cybersecurity or gaming.) AT LEAST 2 must be experts/ have significant experience in ethics DIRECTLY related to your company's tech sector.]

Bruce Schneier (Cybersecurity Expert, Harvard) Bruce is a world renowned cryptographer and security expert. He has written extensively about the ethical responsibilities of cybersecurity. He would bring tons of expertise in encryption and ethics, ensuring our policies remain realistic, effective, and socially responsible without going outside of the scope.

Timnit Gebru (AI Ethics Researcher, Founder of DAIR Institute) Timnit is an important person when it comes to AI ethics. She has published a lot of works on bias, transparency, and the responsible use of AI.Her knowledge would

safeguard ClearAI Security from ethical blind spots and ensure that our AI-driven tools remain fair and just.

Whitfield Diffie (Co inventor of Public Key Cryptography) Whitfield is a pioneer in modern cryptography, whose innovations have brought us secure communication. Having him on the board symbolizes a deep connection to the roots of cryptography while ensuring that our algorithms are held to the highest technical and ethical standards, communicating with the user needs and not just on ours, studying what the market needs

TIPS AT END OF THE SECTION!

4. **Presentation**
5. **References**

[1] ACM. 2018. ACM Code of Ethics and Professional Conduct. Association for Computing Machinery. Retrieved October 2025 from https://www.acm.org/code-of-ethics

[2] Augusta University Online (AU Online). 2025. Cybersecurity Ethics: What Cyber Professionals Need to Know. Augusta University. Retrieved October 2025 from https://www.augusta.edu/online/blog/cybersecurity-ethics

[3] Federal Trade Commission (FTC). 2024. Privacy and Data Security: Protecting Consumer Information. Retrieved October 2025 from https://www.ftc.gov/business-guidance/privacy-security