2. Requirements, Constraints, And Standards

2.1 Requirements & Constraints

The following list of requirements is designed to comprehensively cover all aspects of our project, ensuring alignment with the values placed on user experience, site security, and ease of implementation.

1. Functional Requirements
   - 1.1. Must accurately interpret and respond to user queries. Secure login is also required so experts can vet questions without fear of malicious users having access.
     - 1.1.1. *Amateurs*: Questions are simple and general questions and must be responded to similarly.
     - 1.1.2. *Enthusiasts*: More detailed inquiries that may need diagrams or code snippets to get the point across.
     - 1.1.3. *Experts*: Need backend access through the login system. Intuitive dashboard to vet questions and collaborate with other experts
2. Resource Requirements
   - 2.1. Ensure the vetted answers are stored in the database for future reference, which can be accessed quickly.
   - 2.2. Captain Cyber will need to be able to reference the information stored in the faq, allowing it to bypass expert vetting.
3. User Experiential Requirements
   - 3.1. The interface should be intuitive, and it should take users only a short time to determine how to interact with the Captain Cyber chatbot. The chatbot should also be relatively fast and not take too long to answer questions.
4. UI Requirements
   - 4.1. The color palette of all Captain Cyber-related webpages should match the preexisting colors to promote experience continuity.
5. Security Requirements
   - 5.1. Any user information must be properly hashed and stored with standards up to date with ISU standards.
   - 5.2. The database must be up to ISU standards and potentially even higher.
   - 5.3. User input must be fully or partially sanitized to ensure no malicious or irrelevant input.
   - 5.4. Ensure ambassador questions are relevant and nonmalicious. Security overall must also not constrain the app too much.
6. Performance Constraints
   - 6.1. Responses that do not need to be vetted by experts should not take long to be generated to promote a seamless user experience..

2.2 Engineering Standards

After reviewing the *IEEE Standards in Everyday Life* it is evident that engineering standards are present in our daily lives. These standards ensure that everything we interact with is up to a certain specification that not only provides the best experience but protects us from things we might not consider. From the moment you wake up, your alarm system and cell phone have been met to the *IEEE 802.15 Family of Standards* that focuses on wireless specialty networks (WSNs) and wireless personal area networks (WPANs) that we don't even realize. These standards take on more responsibility as they protect our homes, networks, and essential home utilities such as our water and electricity meters (*IEEE 1701, 1702, 1704 & P13777* are all used for smart metering). As our lives continue, IEEE standards are present in autonomous vehicles and the factories manufacturing everything we need to make it through our day. Overall, standards are set to protect us and ensure we don't have to question the integrity of our essential interactions with various devices.

Based on the *IEEE Interactive Soccer Stadium*, we can see a more in-depth view of standards used in large-scale operations such as sporting events at large stadiums or venues. Take performance and health tracking, for example. For wearable technology to enhance player safety, it must meet *IEEE P3141 for 3D Processing, IEEE 1708 for Wearable Cuffless Blood Pressure Measuring Devices, and IEEE 11073 Family for Health Informatics*. These standards ensure that coaches and trainers can make smart decisions based on the information they get from watching the game. All three of these standards are necessary just for a wearable performance and health tracker. Once we start to think about how many devices we interact with on a day-to-day basis, we will start to realize how much work, research, and development has gone into providing the best experience possible.

It is obvious that these standards are necessary to both protect us and give us the best user experience possible. Without them, there would be consistent errors or outages in vital instruments that keep our society functioning. Thanks to the determined teams at *IEEE,* we have set baselines that must be met for any product or service to make its way to the public environment. It is our duty as engineers to rigorously align our projects to these specifications to uphold the consistent reliability and sustainability of all things digital.

It is important to know that we also must ensure our project abides by all IEEE standards relating to the technologies we will utilize. As the product of rigorous research, we have determined the following standards to directly relate to our project:

IEEE Standard for Large Language Model (LLM) Agent Interfaces IEEE P3394

This standard is focused on defining interactions with AI models. It defines protocol methods and formats for communication between the AI and the system. With this in mind, its main goal is to make AI and system integration as smooth as possible.

IEEE Standard for Artificial Intelligence (AI) Model Representation, Compression, Distribution, and Management IEEE 2941

This standard focuses on the compression and distribution of AI models. It provides guidelines on storage and management. These guidelines and focuses help with the goal of making AI models effective and interchangeable across different types of hardware and software environments.

IEEE Standard for Password-Based Public-Key Cryptographic Techniques IEEE 1363.2-2008

This standard focuses on techniques for cryptographic protocols implementing public-private key encryption. Its goal is to make this type of encryption more secure and easier to integrate when needed.

After reviewing each standard, we have determined they are directly applicable to our project in multiple ways:

IEEE Standard for Large Language Model (LLM) Agent Interfaces IEEE P3394 fits firstly because we are incorporating an AI into Captain Cyber so we need to make sure our system is set up to work smoothly with the AI. Secondly, we need to make sure the AI-incorporated system is able to send and receive data with the format we chose.

IEEE Standard for Artificial Intelligence (AI) Model Representation, Compression, Distribution, and Management IEEE 2941 is also associated with our project since it provides guidelines for managing the AI technology we will implement. It also discusses the API framework for large-scale pre-trained AI models,

which is directly what we will be utilizing in our project. By aligning ourselves with the goals of this standard, we can help promote operational efficiency and proper usage of Captain Cyber.

IEEE Standard for Password-Based Public-Key Cryptographic Techniques IEEE 1363.2-2008 fits because we intend to use public and private key pairs for our ambassadors to log in and respond to asked questions, and this standard will help with its integration into our system. Secondly, it will help ensure that our data can't be stolen by any bad actors praying on the site.

Q4) Review with your team the standards that each of you has selected. What other standards did some of your team members choose that are different?

Some other standards found by the team are IEEE 7000-2021: AI Ethical System Design and IEEE 23026-2023: International Standard - Systems and Software Engineering – Engineering and Management of Websites for Systems, Software, and Services Information. We believe these standards can also align with *Ask Captain Cyber* quite well. However, to access the IEEE 23026-2023 standard, we would have to purchase it to really dive deep into the specificities, but we can potentially incorporate it as we see fit. For the IEEE 7000-2021 standard, we came to the conclusion that we will be implementing this with the other AI-specific standards we have listed above.

In order to meet the specifications required by these standards, we will have to modify our approach to be incredibly detailed. For example, we will have to construct our chat responses and interactions to meet *IEEE P3394* so that the system as a whole runs smoothly without failure. As the focus of *Ask Captain Cyber* revolves around providing expertly vetted answers to cyber-security questions, one of the most important things to realize is that we have to keep our backend secure so that no one with malicious intent can distribute incorrect information. To ensure this happens, we have to abide by *IEEE 1363.2-2008* so that there is no risk of our expert's passwords being leaked or guessed. As we are still in the early stages of development, we won't have to modify any pre-existing systems we have already built; instead, we must work and design with the intent to fulfill all of these standards' needs so that we don't have to regress further down the road. If we can act proactively compared to reactively, we can be sure that *Ask Captain Cyber* is up to specification instead of reconfiguring it to meet the standard.