**Software Requirements Specification (SRS) Document: Center for Cyber Security and Cryptology Institute Website**

1. **Introduction**

**1.1. Purpose**

The purpose of this document is to provide a detailed specification for the development of a website for the Center for Cyber Security and Cryptology. This website will serve as an interactive platform for users to access information about the institute, its services, courses offered, research publications, events, and resources related to cyber security and cryptology.

**1.2. Scope**

The website aims to cater to the following primary objectives:

* Provide an overview of the Center for Cyber Security and Cryptology Institute and its mission.
* Present information about the various courses, programs, and certifications offered in the field of cyber security and cryptology.
* Showcase research publications, articles, and case studies conducted by the institute.
* Announce and manage events including seminars, workshops, and conferences.
* Offer resources such as e-books, tutorials, and tools related to cyber security and cryptology.
* Enable students and professionals to interact with the website by registering for courses, submitting inquiries, and accessing personalized information.

**2. Functional Requirements**

**2.1. User Registration and Authentication**

* The website shall allow users to create accounts and register as students, professionals, or guests.
* Users shall be able to authenticate themselves using a username and password combination or via social media accounts.
* Student and professional accounts shall require additional information such as matricule, educational background and work experience.

**2.2. Programme Information**

* The website shall provide a comprehensive list of programmes offered, including their descriptions, duration, prerequisites, and schedule.
* Users shall be able to browse and search for programmes based on different criteria such as names, fees, and certifications.
* Each programme shall have a dedicated page with detailed information, including outlines, learning outcomes, and fees if applicable.

**2.3. Events Management**

* The website shall have a dedicated section to showcase upcoming and past events organized by the institute, including seminars, workshops, and conferences.
* Events shall be displayed with relevant details such as date, time, location, and registration information.
* Users shall be able to register for events through the website, and event coordinators shall have the ability to manage event registrations.

**2.4. Research Publications**

* The website shall provide a repository of research publications, articles, and case studies conducted by the institute.
* Publications shall be categorized based on topics and authors, and users shall be able to search and filter publications based on these categories.
* Full-text PDF versions of publications shall be available for download or viewing if any.

**2.5. Resources**

* The website shall offer a collection of resources related to cyber security and cryptology, including e-books, tutorials, and tools for students.
* Resources shall be categorized based on topics and shall be searchable and accessible to registered users.

**2.6. Contact and Inquiry**

* The website shall provide a Q&A furum where users can submit questions related to the center or cuver security and experts or any other person having an account on the website can provide answers and engage into a conversation or discussion with users
* Users can upvote or down vote answers to highlight helpful contribution
* In addition to the Q&A furum, the website shall provide contact information for the institute, including email addresses, phone numbers, and physical address of the school and program coordinator for further inquiries.

**3. Non-functional Requirements**

**3.1. User Interface**

* The website shall have a user-friendly and responsive interface that is accessible across different devices, including desktops, tablets, and smartphones.
* The design shall follow a clean and professional aesthetic, with clear navigation and intuitive interaction elements.

**3.2. Security**

* The website shall implement appropriate security measures to protect user data and prevent unauthorized access.
* User passwords shall be securely hashed and stored.
* Sensitive information transmitted over the website, such as during the registration process, shall be encrypted using secure protocols (e.g., HTTPS).

**3.3. Performance**

* The website shall have a fast loading time to ensure a smooth user experience.
* The website shall be able to handle a large number of simultaneous users without significant performance degradation.
* Code optimization and caching techniques shall be employed to enhance the website's performance.

**4. Constraints**

* The website shall be developed using modern web technologies and frameworks, ensuring cross-browser compatibility.
* The development shall adhere to any branding guidelines and visual identity provided by the university.
* The website development shall take into consideration any specific hosting requirements or limitations imposed by the university's IT infrastructure.

**5. Assumptions and Dependencies**

* The development team assumes that the necessary resources and information about the Center for Cyber Security and Cryptology, its courses, events, and research publications will be provided by the center
* The website will depend on an internet connection to function properly.