## Request for Proposal (RFP) for Website Development for Cyber Division in Kerala Police

### 1. Introduction

The **Cyber Division in Kerala Police** is seeking proposals from qualified web development agencies to design, develop, and maintain a bilingual dynamic website. The website will serve as an online platform to disseminate information, enhance public engagement, and showcase the initiatives, operations, and services provided by the Cyber Division. The design and structure should be modern, user-friendly, and align with the objectives of the division.

### 2. Objectives

The primary objective of the website is to provide comprehensive information to the public, law enforcement, and related stakeholders on cyber security, cybercrime prevention, and the services offered by the various divisions of the State Cyber Division. The website should:

- Be a central hub for information, resources, and news related to cyber security and cybercrime prevention.
- Facilitate links for online reporting mechanisms to the public.
- Provide real-time updates on cyber threat alerts and security guidelines.
- Showcase collaboration between the State Cyber Division and other agencies, both national and international.

### 3. Scope of Work

The website should need to include, but is not limited to, the following functionalities:

- **Home Page**: An inherent landing page showcasing the core functions, news updates, and announcements.
- **About Us**: Information about the State Cyber Division, its mission, and vision.
- **News & Updates**: Regular updates on cyber security events, news, and alerts.

- **Reporting Portal**: An interactive portal for citizens to report directly, with a user-friendly form interface.
- **Resources**: A section with downloadable resources, guides, and tutorials related to cyber security and safe online practices.
- **Contact Us**: An easy-to-navigate contact form and directory of important contacts.
- **Links to Other Authorities**: Direct links to national bodies such as **I4C, CERT-IN** and other relevant state and national organizations.
- **Public Awareness Campaigns**: Information and media related to on-going and upcoming public awareness campaigns on cyber safety.
- **Real-time Updates & Alerts**: Integration with other application having a feature to provide users with cyber alerts and updates on real-time security risks.
- **Social Media Integration**: Links to the Division's social media accounts for wider outreach.
- The exact menu structure will be shared post issuance of the work order, and the proposed website must include functionality to dynamically manage both the menu and associated pages.
- The proposed website should generate comprehensive reports, including user activity, cybercrime statistics, public awareness and engagement metrics, system usage and performance, feedback and query responses, news and updates summaries, training and capacity building reports, as well as content management and update logs. These reports should be customizable and available for periodic review to ensure effective monitoring of the website's functionality and user engagement.

## 4. Design and Technical Requirements

- **Design Language**: Design the website with a focus on a clean, modern, and responsive layout that offers high visual appeal, usability, accessibility, SEO optimization, and security. Ensure it provides a superior user experience and maintains functionality across multiple devices, including mobile, tablet, and desktop.

- **Content Management System (CMS)**: The website must be built on an easy-to-manage to allow division staff to make updates without extensive technical knowledge.
- **Security**: The website must be built with strong security measures, including implement OWASP best practices to ensure robust application security, including protection against the top ten most critical security risks.
- **SEO & Analytics**: The website should be optimized for search engines and integrated with tools such as Google Analytics for monitoring site traffic and user behaviour.
- **Multilingual Support**: Support for multiple languages, particularly English and the local state language (Malayalam).
- **Compliance**: The website must comply with **Government of India's Website Guidelines**, including accessibility and security standards.

## 5. Deliverables

- Fully functional and secure website for the State Cyber Division.
- Administrative and user manuals for website management.
- Post-launch support for a period of at least 36 months.

## 6. Budget

The proposal should include a detailed breakdown of costs associated with:

- Website design, development, Hosting and Training.
- Maintenance and support for a minimum of 36 months post-launch.

## 7. Contact Information:

For any inquiries or clarifications regarding this RFP, please contact to Mr. Abdul Rassi .A (9895258496 / 9497936102) or Email: "cyberops-sec.pol@kerala.gov.in".

*********