# RULES FOR ISSISSION HACKATHON

## 

## MARCH 4,5,6

(MARCH 4,5 -OFFLINE, MARCH 6 -ONLINE)

#### **TRACKS**

Coding Track: participants will create software solutions or apps to solve from a given list of problem statements.

Hacking Track: participants will identify vulnerabilities in a simulated system.

#### <u>ROUNDS</u>

Round 1: online coding or hacking challenge to be completed in teams of 2.

Round 2: team-based coding or hacking challenge where teams will compete against each other.

# RULES

## GENERAL RULES

Participants must register individually.

Participants will compete in teams of 2.

All participants will be added to a WhatsApp group.

A Google Form will be shared on March 4 at 12AM and is to be filled by participants by March 4 at 12 PM.

Any violation of the rules may result in disqualification from the competition.

# RUES

## CODING TRACK

#### **ROUND 1**

Participants will be provided with a set of problem statements on the day of the event.

Participants must create an app or wireframe or prototype to solve one of the problem statements provided.

Participants must bring their own laptops and can work individually or in teams of two.

The app or prototype must be original work and not copied from any other source. The app or prototype must be functional and solve the problem statement provided.

The judges will evaluate the submissions based on the following rubrics:

Problem statement understanding and relevance

User interface design

User experience

**Creativity and innovation** 

Functionality and completeness of the solution

The judges' decisions are final and cannot be contested.

# 

## HACKING TRACK

#### **ROUND 1**

Participants must bring their own laptops.

Participants must not cause any damage to the provided system.

Participants must not share any information about the vulnerabilities they find.

Participants must submit their findings through the online platform provided.

The winner will be the participant who finds the most vulnerabilities and exploits them to gain access to the sensitive information.

# RULES

### IT SECURITY MANAGER

#### **ROUND 2**

The second round of the event will take place offline on March 6. Finalists will pose as an Information Security Manager at an Indian bank and will face a randomly chosen incident from a list of four possible incidents. They will have to write a report that includes a standard framework and compliance policies. The reports will be judged, and the top three winners will be announced on March 9.

#### <u>RULES</u>

Finalists will be given a randomly chosen incident to analyze and report on.

Reports should include a standard framework and compliance policies.

The judging panel will evaluate reports based on predetermined criteria.

Top 5 finalists from each stream will move on to the final round.

ChatGPT cannot be used in this phase.

This round will be offline from 4:30PM to 6:15PM and participants are to bring their own laptops and internet.