



Incident Response Team

Established
March 18, 2023

The Eye, CSEA

Dear Team,

Welcome to "The Eye," our cybersecurity club's Incident Response Team (IRT) wing. The IRT team's primary goal is to respond to cybersecurity incidents, cyberbullying/abuse incidents, and work as a CERT (Computer Emergency Response Team) for our college by reverting to any vulnerabilities found on the college website.

Cybersecurity incidents refer to any unauthorized access, data breaches, malware attacks, or any other security incidents that can affect the confidentiality, integrity, and availability of information. The IRT team will respond promptly to any such incidents, investigate the source, and take appropriate measures to contain and remediate the situation. The team will also document the incident and provide a report to the relevant college departments and authorities.

Cyberbullying/abuse incidents refer to any malicious and offensive behavior on the internet, such as harassment, bullying, and other types of abuse. The IRT team will investigate any such incidents and take appropriate action to stop the behavior and provide support to the victims. The team will also educate the college community about the dangers of cyberbullying and how to prevent and report it.

Working as a CERT for our college means that the IRT team will identify and report any vulnerabilities found on the college website. The team will also provide recommendations and best practices to mitigate and prevent future vulnerabilities.

The IRT team takes its role seriously and strives to maintain the confidentiality, integrity, and availability of all information it handles. Confidentiality means that any information related to incidents or victims must remain private and secure. Integrity means that the team must ensure the accuracy and completeness of all information. Availability means that the team must ensure that information is available to those who need it when they need it.

To ensure the success of our team, we have established some guidelines that must be followed at all times. These guidelines are as follows:

1. Team Goals: Our team's goals are to prevent, detect, respond to, and recover from any cybersecurity incidents that may affect our college. We aim to educate the college community about cybersecurity and to foster a culture of security awareness.
2. Confidentiality of Information: The IRT team must maintain strict confidentiality regarding any information related to cybersecurity incidents. This includes personal information of individuals involved in the incident, technical details, and any other sensitive information. All team members must sign a confidentiality agreement before joining the team.
3. Ensuring CIA Triad: Our team is committed to ensuring the CIA triad of confidentiality, integrity, and availability for all college information systems. This means that we must protect information from unauthorized access, ensure the accuracy and completeness of information, and ensure that information is available when needed.
4. Reporting incidents: Any member of the college community who suspects a cybersecurity incident must report it to the IRT team immediately. The team will investigate the incident and take appropriate action. All team members must document their activities and provide regular updates to the team lead.
5. Collaboration: The IRT team must work collaboratively with other college departments, such as IT, HR, and legal, to respond to incidents effectively. The team must also collaborate with external organizations, such as law enforcement agencies and other CERTs, as needed.
6. Training and Development: All IRT team members must receive training on cybersecurity incident response, cybersecurity best practices, and relevant laws and regulations. The team must also engage in ongoing professional development to stay up-to-date with the latest threats and trends in cybersecurity.

In summary, our IRT team is responsible for responding to cybersecurity incidents, cyberbullying/abuse incidents, and working as a CERT for our college by reverting to any vulnerabilities found on the college website. We must maintain the confidentiality, integrity, and availability of all information we handle and follow the guidelines outlined in this document. We are committed to ensuring the security and safety of our college community and educating them about cybersecurity best practices.

Sincerely,
Aaditya Rengarajan
IRT Team Lead