RFC 2350 EDU-CSIRT KEMENDIKBUDRISTEK

1. Information regarding this document contains a description of the Edu-CSIRT of the Ministry of Education, Culture, Research and Technology (Edu-CSIRT Kemendikbudristek) based on RFC 2350, which is basic information regarding the Edu-CSIRT of the Ministry of Education, Culture, Research, explaining responsibilities, services provided, and ways to contact the Edu-CSIRT of the Ministry of Education, Culture, Research and Technolgy.
   1.1. The last update date of the document is version 1.2 of the document issued on March 2, 2023
   1.2. There is no distribution list for notification of document updates.
   1.3. The location where this document can be found. The latest version of this document is available on the web https://educsirt.kemdikbud.go.id.
   1.4. The authenticity of the two documents (English and Indonesian versions) is a document that has been signed by the Head of the Center for Data and Information Technology (PUSDATIN) of the Ministry of Education, Culture, Research and Technology.
   1.5. The document identification of both documents (English and Indonesian versions) has the same attributes, namely:
      1.5.1. Title: RFC 2350 EDU-CSIRT KEMENDIKBUDRISTEK
      1.5.2. Version: 1.2
      1.5.2. Published Date: March 2, 2023
      1.5.3. Expiration: This document is valid until the newest document is published.

2. Data / Contact Information
   2.1. The name of the Education-Computer Security Incident Response Team of the Ministry of Education, Culture, Research and Technology is abbreviated as Edu-CSIRT Kemendikbudristek.
   2.2. Address of the Center for Data and Information Technology Kemendikbud Jl. RE Martadinata Cipayung, Ciputat, South Tangerang, Banten, Indonesia.
   2.3. Jakarta Time Zone (GMT + 07: 00)
   2.4. Telephone Number (021) 7418808,
   2.5. Fax Number (021) 7401727
   2.6. Helpdesk Number of Edu-CSIRT Kemendikbudristek 08111977478
   2.6. E-mail address educsirt [at] kemdikbud.go.id

2.7. Team Members

The Chairperson of the Edu-CSIRT Kemendikbudristek is the Head of the Ministry of Education, Culture, Research and Technology's Information Technology (Pusdatin) with team members, all staff in the application and information security, Information Technolgy governance, Data and Education Statistic, Cultural and Linguistic dDta and Representatives of the work units in the Kemendikbudristek.

2.8. Other information / data Not available.

2.9. Notes on Contact Edu-CSIRT Indonesia

The recommended method for contacting the Edu-CSIRT Kemendikbudristek is via e-mail at educsirt [at] kemdikbud.go.id address or via telephone number (08111977478) to the EDU CSIRT Kemendikbudristek which is on standby 24/7.

3. Regarding the Edu-CSIRT

3.1. The vision of the Edu-CSIRT Kemendikbudristek is the realization of cyber resilience in a reliable and professional education sector.

3.2. The missions of the Edu-CSIRT Kemendikbudristek are:

3.2.1. Coordinating and collaborating cybersecurity services in the government sector, especially the education sector, both internal and external

3.2.2. Thoroughly identifies security vulnerabilities

3.2.3. Increasing security aspect response to all MOEC Work Units

3.2.4. Improve the quality of educational and cultural ICT services from cyber threats.

3.3. Constituents

The constituents of Edu-CSIRT Kemendikbudristek are all units of the Ministry of Education, Culture, Research and Technology.

3.4. Sponsorship and / or Affiliates

Sponsorship and / or Edu-CSIRT Affiliation Kemendikbudristek is part of the Ministry of Education, Culture, Research and Technology's Pusdatin so that all funding comes from the APBN.

4. Policies

4.1. Types of incidents and levels / levels of Edu-CSIRT Kemendikbudristek Supports to handle incidents, namely:

a. Web Defacement;

b. DDoS;

c. Malware;

d. Phishing;

e. Account hijacking

f. Illegal Access

g. Spam

The support provided by Edu-CSIRT Kemendikbudristek to constituents may vary depending on the type and impact of the incident.

4.2. Cooperation, Interaction and Disclosure of Information / data

Edu-CSIRT Kemendikbudristek will collaborate and share information with CSIRTs from other Ministries and / or Institutions within the scope of cybersecurity. All information received by the Edu-CSIRT Kemendikbudristek will be kept confidential.

4.3. Communication and Authentication for regular communication The Edu-CSIRT Kemendikbudristek can use an e-mail address without data encryption (conventional e-mail) and a telephone.

5. Service

5.1. Reactive Service

Reactive services from the Edu-CSIRT Kemendikbudristek are the main and priority services, namely:

5.1.1. Alert service related to cyber incident reports

This service is carried out by the Edu-CSIRT Kemendikbudristek in the form of providing warnings of cyber incidents on electronic systems and statistical information that are managed by each Ministry of Education, Culture, Research and Technolgy work unit.

5.1.2. Incident response and recovery services

This service is provided by Edu-CSIRT Kemendikbudristek in the form of coordination, analysis, technical recommendations, and site visit assistance in the context of cyber incident prevention and recovery. The Edu-CSIRT Kemendikbudristek provides statistical information regarding this service.

5.1.3. Vulnerability handling services

This service is provided by the Edu-CSIRT Kemendikbudristek in the form of coordination, analysis and technical recommendations in the context of strengthening security (hardening), the Edu-CSIRT Kemendikbudristek provides statistical information regarding this service. However, this service is only valid if the following conditions are met:

a. The reporter for vulnerability is the owner of the electronic system. If the reporter is not the owner of the system, then the vulnerability report cannot be handled;

b. The vulnerability management service in question can also be a follow-up to the Vulnerability Assessment activity.

5.1.4. Artifact handling services

This service is provided by the Edu-CSIRT Kemendikbudristek in the form of handling artifacts in the context of restoring the affected electronic system or supporting investigations. Edu-CSIRT Kemedikbudristek provides statistical information regarding this service

5.2. Proactive Service

Edu-CSIRT Kemendikbudristek is actively building the capacity of cybersecurity resources through the following activities:

5.2.1. Notification of the results of observations related to new threats. This service is provided by the Edu-CSIRT Kemendikbudristek in the form of results from the early detection system of the security monitoring system. The Edu-CSIRT Kemendikbudristek provides statistical information regarding this service.

5.2.2. Security assessment service

This service is provided by the Edu-CSIRT Kemendikbudristek in the form of vulnerability identification and risk assessment of the vulnerabilities found. The Edu-CSIRT Kemendikbudristek provides statistical information regarding this service.

5.2.3. Security audit service

This service is provided by Edu-CSIRT Kemendikbudristek in the form of an information security assessment. The Edu-CSIRT Kemendikbudristek provides statistical information regarding this service.

5.2.4. Management Services

Quality of Security Edu-CSIRT Kemendikbudristek improves the quality of security through the following activities:

a. Consultation related to incident response and recovery readiness

b. This service is provided by the Edu-CSIRT Kemendikbudristek in the form of providing technical recommendations based on the results of analysis related to incident response and recovery.

c. Building cybersecurity awareness and concern

d. In this service the Edu-CSIRT Kemendikbudristek documents and publishes various activities carried out in the context of building awareness and concern for cybersecurity.

e. Coaching related to incident response and recovery readiness

f. Edu-CSIRT Kemendikbudristek prepares a coaching program in order to support incident response and recovery

6. Incident Reporting

   Cybersecurity incident reports can be sent to educsirt [at] kemdikbud.go.id by attaching at least:

   a. Photo / scan of ID card

   b. Evidence of the incident in the form of photos or screenshots or log files found

7. Disclaimer regarding the handling of this type of malware depends on the availability of the tools that are owned.