Users of different systems working on various platforms and using different applications may report any vulnerability found in these systems, platforms, applications, services and devices to CERT-MU.

An incident can be reported to CERT-MU as follows:

- **Website**
  The incident can be reported by filling up the incident reporting form on our website (www.cert-mu.org.mu) and fill in as many fields as possible to enable CERT-MU to assess the severity and nature of the incident and assist in recovery, as needed.

- **Electronic Mail**
  The CERT-MU email address for reporting incidents is: incident@cert-mu.gov.mu
  For all other inquiries and correspondence, write to: info@cert-mu.gov.mu
  Occasionally, a compromised system’s electronic mail may be under surveillance by the intruder. If that is suspected, you are advised to use other means (telephone: 800 2378) to file your report.

- **Telephone**
  You can contact the CERT-MU Team on the toll free number: 800 2378
  Business hours: 8:45 am to 4 pm

**How to report a vulnerability to CERT-MU**

A vulnerability can be reported to CERT-MU by filling up the Vulnerability Reporting Form provided on our website. The information about a particular vulnerability can also be sent to CERT-MU by e-mail: info@cert-mu.gov.mu

**Contact information**

CERT-MU
National Computer Board
7th Floor, Stratton Court
La Poudrière Street
Port Louis
Mauritius

Toll Free Number: 800 2378
Email: info@cert-mu.gov.mu
Web: www.cert-mu.org.mu
Fax: 208 0119
1. WHAT IS CERT?

Computer Emergency Response Team (CERT) acts as a trusted single point-of-contact clearinghouse dealing with Internet security problems and providing services which includes 24-hour technical assistance for responding to computer security incidents, product vulnerability assistance, technical documents and training on information security issues.

In the World Summit on Information Society Geneva Action Plan of 2003, under Action Line C5, member states were invited to set up focal points for real-time incident handling and response (i.e. CERT), and develop a cooperative network between these focal points for sharing information and technologies on incident response.

CERTs have come into existence in almost every part of the world today (e.g. Australia, Brazil, China, European countries, India and USA). African countries such as South Africa, Kenya and Tunisia have already set up their CERTs.

2. WHAT IS CERT-MU?

CERT-MU is an acronym for ‘Mauritian Computer Emergency Response Team’. CERT-MU has been set up by the National Computer Board (NCB) :

- for the monitoring of the information security situation at the national level,
- for dissemination of advisories vulnerability notes and alerts on latest information security threats, countermeasures and best practices,
- for management of information security risks including the reporting of information security breaches and incidents and
- to be part of the international CERT community.

3. MISSION OF CERT-MU

The CERT-MU’s mission is:

To provide information and assistance to its constituents in implementing proactive measures to reduce the risks of information security incidents as well as responding to such incidents when they occur.

4. CERT-MU SERVICES

- Issuing of Information Security alert which includes advisories, vulnerability notes and virus alerts.
- Incident response and coordination for the entire cyber community of Mauritius
- Information Security awareness programme which includes workshops and trainings on Information Security themes.
- Assistance to organisations in the implementation of Information Security Management System (ISMS) based on ISO 27001 standard.
- Vulnerability Scanning Service.

5. CONSTITUENCY

CERT-MU’s constituency is the entire cyber community of Mauritius.

CERT-MU will receive intrusion attempts reports, virus incidents and other security problems from defined staff of each Constituent within each institution, namely Security Contact Person(s).

6. INCIDENT REPORTING

CERT-MU addresses all types of computer security incidents, which occur at its constituency.

CERT-MU may act upon requests of one of its constituents or may act if one of its constituents is involved in a computer security incident.

The level of support given by CERT-MU will vary depending of the type and severity of the incidents or issue, the size of the user community affected and the CERT-MU’s resources at the time which occurs at its constituency.

Users and System Administrators can report computer security incidents and vulnerabilities to CERT-MU.

If you encounter any of the violations given below, you may contact CERT-MU for technical assistance:-

1. Attempts (either failed or successful) to gain unauthorised access to a system or data therein
2. Disruption or Denial of Service
3. Unauthorised use of a system for the processing or storage of data
4. Changes to system hardware, firmware, or software characteristics without owner’s knowledge, instruction, or consent
5. Email-related security issues, spamming, mail bombing etc.
6. Attempts for Identity theft such as phishing
7. Unauthorised modification of website content, defacement, injection of Malicious links etc.