CERT - MU

Incident Reporting Form

Kindly complete this form and submit to CERT-MU

All fields marked with * are mandatory and must be filled in.

1. Contact Information of Reporting Party: *

Name:

Organisation:

Title:

Address:

Email:

Telephone No:

Fax No:

Mobile No:

2. Sector of Reporting Party: *

☐ Government ☐ Financial ☐ Utilities ☐ Tourism ☐ Transportation ☐ Manufacturing

☐ Health ☐ ICT ☐ Academia ☐ Telecommunications ☐ Other

3. Location of Affected Computer/Network

Location:

4. Date and Time incident Occurred:

Date:

Time:

5. Symptoms of Incident: *

☐ System crashes

☐ New user accounts/ Accounting discrepancies

☐ Failed or successful social engineering attempts

☐ New files

☐ Changes in file lengths or dates

☐ Attempts to write to system

☐ Data modification or deletion

☐ Denial of service

☐ Unexplained, poor system performance

☐ Anomalies

☐ Suspicious probes/Scanning

☐ Suspicious browsing

☐ Unaccounted for changes in the DNS tables, router rules, or firewall rules

☐ Unexplained elevation or use of privileges

☐ Operation of a program or sniffer device to capture network traffic;

☐ Unusual time of usage

☐ An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user

☐ Unusual usage patterns

☐ A system alarm or similar indication from an intrusion detection tool

☐ Unusual log file entries

☐ Presence of new setuid or setgid files

☐ Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server

☐ Presence of cracking utilities

☐ Activity during non-working hours or holidays

☐ Others (Specify)

6. Type of Incident: *

- ☐ Phishing
- ☐ Virus / Malicious Code
- ☐ Network Scanning / Probing
- ☐ Web Site Defacement
- ☐ Intrusion
- ☐ Break - in / Root Compromise
- ☐ Spam
- ☐ Email Spoofing
- ☐ Denial of Service
- ☐ Others (Specify)
- ☐ System Misuse
- ☐ Social Engineering
- ☐ Technical Vulnerability
- ☐ User Acount Compromise
- ☐ IP Spooling

7. Description of Incident:

8. Additional information of affected system (OS, Application Software, Patch Level, etc):

9. Agencies Notified?

☐ Law Enforcement ☐ Private Agency ☐ Affected Product Vendor ☐ Other

10. Approximately how many systems were affected?

The CERT-MU address for reporting incidents:

Email Address: incident@cert-mu.gov.mu

Postal address: CERT-MU
C/o Government Online Centre
5th Floor
Cyber Tower,
Ebene, Mauritius

Fax No: 467 5421