

**PROCEDURES FOR:
Network Engineers and Server Administrators
ACTIVATING THE COMPUTER SECURITY INCIDENT
RESPONSE TEAM (CSIRT)**



Description:

Suspected computer security incidents and confirmed incidents can be sensitive in nature and need to be handled professionally and with care. Please limit any discussion regarding incidents to those individuals directly involved.

Everyone involved should do their best to remain calm and professional while investigating suspected incidents. The main objectives of CSIRT are to:

- Provide first response.
- Preserve the evidence.
- Contain the problem.
- Guard information about the case and limit discussions to CSIRT, the computer owner, and the individual(s) reporting the incident, if applicable.
- Track and record the incident using Magic.

You should activate CSIRT:

- If a computer with a Mason IP address is probing either another Mason computer or a computer offsite (off-campus incidents are often reported via StopIt or abuse@gmu.edu).
- If a compromised computer is suspected or confirmed to contain highly sensitive data.

What to do:

1. If you are able to identify the location or owner of the computer, create a Magic ticket and use the CSIRT category. NOTE: If you cannot create a Magic ticket, please see “What to do (non-Magic)” section below.
2. If you cannot identify the location or owner of the computer, please contact the Network Operations Center (NOC) for immediate assistance with identifying the suspected computer’s location. The NET (Network Engineering Team) should provide the IP and/or Mac address, building location, telecom room and switch port and forward any log files that may assist in the investigation. NET should disable (partition) the port if appropriate.
3. Alert via telephone by speaking with one of the CSIRT Techs (see list below) so they know they are being activated pending the identification of a suspected computer’s building location.

**PROCEDURES FOR:
Network Engineers and Server Administrators
ACTIVATING THE COMPUTER SECURITY INCIDENT
RESPONSE TEAM (CSIRT)**



What to do (non-Magic):

1. Please collect the following information and e-mail it to CSIRT-1@listserv.gmu.edu:
 - The time and date when the potentially significant security incident occurred.
 - The identities of computers suspected of being compromised by providing the IP and/or Mac address, building location, telecom room and switch port and forward any log files that may assist in the investigation.
 - A brief summary of what is happening (e.g., unauthorized access attempts successful/unsuccessful).
 - If known, please include the user, system owner, and/or administrator of any computers related to the computer generating the attack or the victim of the attack.
2. Alert by telephone by speaking with one of the CSIRT-Techs so they know the email is on its way. See list below.

CSIRT Techs

Mike Bellinghoven, Manager	571-274-2735
Adnan Hameed	571-274-2744
Sunil Sharma	571-274-2742
Adam Curtis	571-237-8554