

**PROCEDURES FOR:
The Computer Security Incident
Response Team (CSIRT)**



REPORTING A SUSPECTED ELECTRONIC SECURITY INCIDENT

Description:

CSIRT should be activated:

- 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. Make an image of the computer.
2. Speak with one of the CSIRT Decision-makers by telephone. Alerting them that the investigation has begun (see list below).
3. Document everything using the CSIRT report form (posted on DocuShare in IT Security Office section under “CSIRT”).
4. Take care with the original hard drive — it must be handled carefully (this is the primary evidence). Document each step in how the original hard drive is handled. Be sure to lock up the original hard drive when not examining it until the CSIRT Executive advises you to return it to the owner.
5. Make a copy of the image so that you can perform forensics on one copy while "preserving the evidence" on the other until the CSIRT executive directs the team to purge the copies.
6. Perform forensics on one of the copies to determine what the compromise is. For example, a worm, spyware, rootkit, trojan, virus, etc.
7. Record your findings on the CSIRT report form. Include any websites or other references you may have discovered that talk more about the threat(s). The report form is designed to (a) document the compromise in case the incident ends up in court and (b) provide the CSIRT Executive with enough information to make University-level decisions.
8. Forward the report to the CSIRT Decision-makers for instructions on how to proceed. Every effort should be made to forward the CSIRT report within 24 hours.¹

CSIRT Decision-makers	
1 st Bob Nakles	703-993-2975
2 nd Walt Sevon	703-993-3548

¹ Commonwealth of Virginia requires that the CIO receive a report within 24 hours of an incident. If CIO and Executives declare it is an incident they will report it to the Virginia Information Technology Agency per the Code of Virginia § 2.2-603.G.