Security Incident Report Form

This form must be completed immediately after the detection of a security incident.

(IR security incidents will be reported and the form completed by the person observing or discovering the occurrence.)

General Information

Name:_____________________________

Department filing report:____________________________________________________________

Location of incident:_________________________________________________________________

Reported by (Name, Title, Location and Department):                                   ______________________________
                                                                                       ______________________________
                                                                                       ______________________________
                                                                                       ______________________________

Date and time of report filing: ___/___/_____

Date and time of incident:      ___/___/_____

Incident Category:

Details of incident (description of the who, what, when, where, how, and why):

The name and title of the person to whom the incident initially was reported to:

______________________________          ______________________________

Identification of appropriate law enforcement organization notified:

____________________________________________________________________
Incident impact on day-to-day operations:

Action taken to contain the incident (note what persons and/or vendors have been contacted):

Short-range corrective action, such as discontinuing the use of an infected computer (Include asset number or account ID):

Long-range corrective actions, as necessary:

Additional information, as appropriate:
Host Information

Please provide information about all host(s) involved in the incident. Please list each host separately.

Computer Name:______________________________________________________________

IP Address:______________________________________________________________

Computer Hardware:______________________________________________________________

Operating System and version:______________________________________________________________

Where on the network is the involved host? (Campus Network, VPN, Home, Shared Space, Lease space):______________________________________________________________

Nature of information at risk on involved host or machine (Student Files, Protected Business Files, Personnel, Financial, Privacy Act):

Was the host the __source __victim __both of the incident?

Was the host compromised as a result of the incident? __yes __no

Hours system / machine down: _________

Incident Categories
(All categories applicable to the incident must be documented)

Data Loss(es):

Hardware Loss(es):

Intruder gained “access”? __yes __no

Administrative password used? __yes __no

Cracked / unprotected password used? __yes __no
Easily guessable password used? __yes  __no

Misuse of host(s) resources? __yes  __no

**Detailed Incident Description**
This should be as detailed as possible, especially when writing lesson learned or after the incident follow-up report. Please create and attach separate Word Document(s) (.doc) to address the following:

A. Duration of incident

B. How was the incident discovered?

C. Method(s) used by intruders to gain access to host(s)

D. Detailed discussion of vulnerabilities exploited that are not addressed in previous sections

E. Hidden files / directories

F. Did the system contain protected information? What type?

G. Were logs being maintained? If so, please describe

H. Were policies and procedures being followed and enforced? (Password / Data Encryption / Hardware Encryption / Anti-Virus / Secure Connection and others as applicable to the host(s) and machine(s)?)
   If so, please describe

*Draft notes: this form will be available on the Information Security web page. An information campaign will be mounted to inform the user community of the guidelines and expectations of all system users. The form will route directly back to Information Security via the Security@cofc.edu email address. It is our intention to create this as a “web form” in the future, to expedite the reporting process.*