DOCUMENT INCIDENT RESPONSE FORM

Stop until instructed to proceed

Contain (Isolate from Network)

Create Forensic Image (if Instructed)

Eradicate

Secure the method of compromise

Recover/Restore the System

Image

Investigate How, What, Where, When & Extent

1

Incident Reported or Discovered

1

Notify: CISO, Director of ITS

Recovery Successful?

NO

YES

YES

Loss of Device?

NO

Suspect Criminal Activity

NO

High Risk Incident?

NO

Low Risk Incident?

NO

Non-significant Incident

YES

YES

YES

Send Copy of Documentation to CISO

Lessons Learned Investigation and Publication

Notify CISO, Campus Police, & Director ITS

Collect Evidence per Law Enforcement Guidance

Contain and eradicate exploit. Recover/Restore the system

NO

Recovery Successful?

YES

Incorporate Lessons Learned into IR process

1

Personal information compromised?

YES

Initiate Information Security Breach Disclosure Process

NO

End

DOCUMENT INCIDENT RESPONSE FORM