Compromised System Procedure

The IT Security Office will need to be notified if any sensitive* information is, or is suspected to be stored directly on the compromised computer(s), network drives, removable drives, etc. that the computer accesses. Please follow the steps below:

1. Disconnect the computer from the network (i.e. pull the network cable from the computer and/or disable wireless).
2. Do not power off, reboot, or reformat the machine until instructed by the IT Security Office.
3. Do not continue to use the machine or make any changes (ex. running anti-virus scans).
4. Contact the Information Technology Security Office (security@fiu.edu, 305-348-1366).
5. If any of the user or service credentials used on the compromised system can be used on any other systems (i.e. the credentials of a staff member’s AD account), those passwords should be changed immediately and the Administrators of the system should be notified.

*Highly Sensitive Data is defined as information which must be protected from disclosure by state or federal law, or by binding contractual arrangement. Among the types of data included in this category are individually identifiable financial or health information, social security numbers, credit card information, student education records and proprietary data protected by law or agreement.