RIT Information Security Office
Computer Incident Response Process
(Laptop or Desktop)

Suspected security incident identified

Loss or theft of device?

No

Notify Public Safety

ISO support needed?

Yes

Decryption Candidate?

No

Contact IT support personnel/ITS Service Desk

IT supports creates forensics image (memory and disk)

ISO conduct investigation/ITS assist ISO investigation as needed

ITS sends forensics image to ISO

IT support creates forensics image (memory and disk)

No

Reimage or remove threat

Restore to service

Exit Computer Incident Response Process

ISO communicate Resolution and lessons learned

Lessons learned

Exit Computer Incident Response Process

For more information, Contact:
Jim Moore, Sr. Information Security Forensics Investigator, direct: (585) 475-5406, e-mail: jhmiso@rit.edu
Paul Lepkowski, Information Security Engineering Manager, direct: (585) 475-6972, e-mail: peliso@rit.edu
Http://www.rit.edu/security

Revised 9/23/14
Version 3.1