ISO Position Paper

Position Title	Device Reimaging
Position Audience	Princeton IT Professionals
Contact	Information Security Office: InfoSec@princeton.edu
Position Release Date	August 10, 2017
Last Update	Initial posting

Problem Statement

Standard anti-virus software does not always detect and protect against today's sophisticated malware. Additional action is needed to guarantee the integrity of devices on which a malware event occurs.

ISO Position

In order to guarantee the integrity of University devices on which a malware event occurs, the ISO requires that the device be reimaged before reconnecting it to the network.

Additional Information

If data has been compromised, please refer to the data breach procedure referenced below:

https://informationsecurity.princeton.edu/sites/informationsecurity/files/PossibleDataBreachProcedure_0.pdf

Information Security Office
Princeton University

Data classification: Public