Data Security Incident Report

Immediately upon discovering a possible data security incident, employees must file a Data Security Incident Report with the College's Information Security Officer. A data security incident would include:

1. Computing Devices Compromised by Malware (when sensitive data is stored on the device, or if you cannot rule out the presence of sensitive data on this device)
2. Computing Devices Compromised by Unauthorized Access (includes any devices accessed without permission, either by stolen or compromised credentials, or other attempts to access a device without authorization)
3. Lost or Stolen Computing Devices

*Computing devices refers to all College-owned computers, servers, portable media, external hard drives or other mobile devices, or personal computing devices containing sensitive College data.

To file a Data Security Incident Report, email ISO@wellesley.edu the following information:

1. Nature of the incident (include approximate date and time the incident occurred, where it occurred, symptoms, how you first responded)

2. Identity Finder and malware scan (Malwarebytes, etc.) results (if available)

3. Whether or not you believe the device contains sensitive information, including Personal Information (PI) or Protected Health Information (PHI).

4. Building and room number

5. Your email address and campus telephone number