CUL Confidential Data Hygiene Procedure
Jun 29, 2015

This procedure outlines how CUL manages compliance with University Policy 5.10 with respect to handling confidential (Level 1) data.

High-Risk Areas

Most staff in CUL have little need in the course of normal business to handle Level 1 data, but there are areas where it is known to be a part of day-to-day business. These areas are at higher risk of noncompliance due to increased exposure. Currently, those areas identified as high-risk are the Finance and Budget Office, and Human Resources.

For the high-risk areas, staff will run the supported data discovery tool (currently Identity Finder) every six months. Supervisors will attest annually that staff are running data discovery and remediating any non-compliant data storage. Desktop Services staff from CUL-IT will be available to provide technical support for the scanning process and any remediation needed, but responsibility for compliance with policy will rest with the unit.

Standard Procedure for Other Areas

For all other areas of CUL, Desktop Services will coordinate scanning of staff workstations on a four-year rotation, covering approximately 25% of staff workstations every year. As with the high-risk areas, Desktop Services will provide technical support for the scanning and remediation process, and supervisors of the selected areas will attest to compliance.

Documentation of Compliance

The IT Security Liaison will collect attestations from supervisors in all high-risk areas and the other areas targeted for scanning in a given year, and report compliance to the AUL for Administration and to the Director of Library Information Technologies.