The CU-Boulder Campus has defined additional requirements beyond the Minimum Security Standards for Networked Devices for systems handling, processing, or storing certain types of data (classified below as Private or Restricted). In some cases requirements will be different for client systems handling data and server systems storing data. Additionally, systems which contain Private data may require compliance verification by a third party as arranged by the Campus Information Technology Security Office.

Private:

Data whose disclosure to unauthorized persons would be a violation of federal or state laws or University contracts. Examples include but are not limited to credit card information, social security number or associated personally identifiable information.

CU-Boulder Private Data Security Requirements

Restricted:

Data which if disclosed without authorization could cause harm or embarrassment to the University or its faculty, students, or staff. Data that would not expose the University to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. An example includes but is not limited to personnel information.

CU-Boulder Restricted Data Security Requirements