**How We Can Limit Access to Systems and Data Based on the User’s Job Roles:**

****

In order to limit access to systems and data based on the user’s job roles, certain restrictions need to be in place. This is to ensure that data is only accessed by those who need it to perform the job. For example, engineers should not have access to fiscal data while financial analysts should. There are various ways to limit access only to systems that are necessary for the user’s job roles. Some examples and implementation ideas are listed below:

* An example is implementing *sharing rules*, also considered as role hierarchies. In this situation, the level of data that a person has is only access that the user needs.
  + Ex. CTO should have access to all admin engineering systems and applications
  + Ex. CFO should have access to all admin financial and accounting data
  + Ex. Contractors should have less access than Chief Officers- only pertaining to accessing systems necessary to fulfill their obligations
* Peer to Peer sharing should be limited to appropriate contacts within the company and approved partners
* In order to protect sensitive information, there will be restrictions on where sensitive files can be saved and accessed
* Peer to Peer networks should be monitored for sensitive information
* *Role based authorization* should be implemented. Commonly used by businesses, this includes the settings of mandatory access control and discretionary access control, serving to restrict system access only to authorized and pre-approved users.

The scope of this policy should apply to

* All institution offices
* Employees, consultants, contractors, agents and authorized users accessing systems and applications
* Applications or systems that store, process, or transmit information such as, network and computer hardware, software and applications, mobile devices, and telecommunication systems