



ACCESS CONTROLS

Right access. Right Purpose. Right People



We practice role-based access.

You can **only** access systems and documents that you need to do your job.

What is ROLE-BASED ACCESS?

Access is granted based on your role and job responsibilities.

If it's not related to your work or you have no legitimate basis, it is **not allowed**.



You cannot access if it is:

- Unrelated to your work responsibilities
- Out of curiosity or for personal reasons
- Without a legitimate business need or proper authorization



You can access if it is:

- Required for your assigned duties
- Needed to perform your work
- Authorize and approved for you



IF YOU DON'T NEED IT, DON'T ACCESS IT.

Respect access. Protect Information. Protect Our Community.

Unauthorized access can lead to

- Violation of Data Privacy Policies
- Unauthorized Disclosure of Sensitive Information
- Disciplinary Action

Do your part

- Access only what you need for your work
- If in doubt, ask. Contact your supervisor or IT security
- Report any unauthorized access or suspicious activity