5 guiding principles for handling data

1. Information Classification
   - Document a company data classification scheme with classification level (e.g., public, internal, secret), definition, examples, and guidelines for accessing, processing, sharing, and storing the data.
   - Don’t forget to classify documents based on the data classification scheme so people will know how to treat them securely.

2. Use approved applications for data storage, and manage the access
   - Always use company approved applications to store your data and files and follow the data classification guidelines.
   - Regularly check and update who needs to have access to the data to perform their job.

3. Sharing data
   - Accessing data
     - Ask the data owner for access to classified documents if needed.
     - Do not bypass primary access controls by sharing data via methods such as E-mail, Zoom, Skype, or Microsoft Teams.
   - Company sanctioned sharing solutions
     - Document and use appropriate company sanctioned sharing methods based on the data classification.

4. Handling requirements for data
   - Do not handle data outside of its approved storage location
   - If you do not have a way to share data within its primary location, limit the risk of unauthorized access by encryption & password protection.

5. Incident management
   - If you suspect unauthorized access to data, submit a security incident as soon as possible and inform your management.