**Access Control Requirements in Online Social Networks**

Access control in social networks refers to the set of policies, rules, and mechanisms that determine who can access or interact with a user’s data, such as posts, messages, images, profile details, and friend lists.

With millions of users sharing personal content on platforms like Facebook, Instagram, and Twitter, there is a need to protect user data from unauthorized access, abuse, or misuse.

**1. User-Centric Access Control**

**Explanation:**

* This requirement focuses on giving users complete control over who can view, interact with, or share their content.
* The system must allow each user to set personalized privacy and sharing preferences for their data.

**Details:**

* Users should be able to set visibility for each post or content item (e.g., public, friends only, private).
* Settings should be easy to access and modify at any time.
* Content-sharing controls should include options to manage tagging, commenting, and sharing.

**Example:**

* In Facebook, when a user uploads a post, they can choose whether it is visible to everyone, only friends, only specific friends, or just themselves.

**2. Relationship-Based Access Control (ReBAC)**

**Explanation:**

* In social networks, users are connected through different kinds of relationships such as friends, followers, or group members.
* Access rights should be based on the nature of the relationship between the content owner and the viewer.

**Details:**

* The system should define access rules like:
  + Only friends can see personal posts.
  + Friends-of-friends may see selected content.
  + Blocked users should not be able to access anything.

**Example:**

* A user on LinkedIn can choose to allow only first-level connections (direct contacts) to see their full profile.

**3. Granular Permission Control**

**Explanation:**

* Users should be able to manage detailed permissions for different actions that others can perform on their content.

**Details:**

* Granular control includes the ability to manage:
  + Who can comment on a post.
  + Who can like or react.
  + Who can share the content.
  + Who can tag the user in posts or photos.
* This level of detail prevents unwanted interactions and maintains user control.

**Example:**

* Instagram allows users to disable comments on individual posts if they want to prevent interaction.

**4. Group-Based Access Control**

**Explanation:**

* Users may want to organize their contacts into groups and apply different access rules to each group.

**Details:**

* Common groups include family, colleagues, classmates, or custom-created groups.
* Access permissions can be assigned to these groups to simplify content sharing.

**Example:**

* A Facebook user might share holiday pictures with only their “Family” group and restrict access from their “Work” group.

**5. Content-Type-Based Access Control**

**Explanation:**

* Social networking platforms allow users to share various types of content. Each type may require different levels of privacy.

**Details:**

* Content types include:
  + Profile pictures
  + Cover photos
  + Friend lists
  + Status updates
  + Birthday or contact information
* The user should be able to configure access settings for each content type separately.

**Example:**

* A user might want to make their profile photo public while keeping their friend list private.

**6. Time-Based Access Control**

**Explanation:**

* In some cases, users may want content to be available only temporarily. Time-based control allows automatic expiration of access.

**Details:**

* Users can set a time limit for content visibility.
* After the time expires, the content is hidden or deleted automatically.

**Example:**

* Instagram Stories disappear after 24 hours. Users do not have to manually delete them.

**7. Blocking and Reporting Mechanisms**

**Explanation:**

* A user should be able to protect themselves from harassment, spam, or unwanted contact by blocking or reporting others.

**Details:**

* Blocking a user should:
  + Prevent them from viewing any content.
  + Stop them from sending messages.
  + Stop them from tagging or commenting.
* Reporting allows users to notify the platform administrators about abusive or suspicious behavior.

**Example:**

* If someone sends inappropriate messages, the victim can block the sender and report their account for review.

**8. Audit Logging and History Tracking**

**Explanation:**

* The system should maintain logs of who accessed what content and when. This helps identify misuse or data breaches.

**Details:**

* Logs may include:
  + Profile view history.
  + Content access records.
  + Login attempts.
* Admins can use these logs for investigations or user complaints.

**Example:**

* If private images are leaked, access logs can help determine which users viewed or downloaded the content.

**Conclusion:** Access control in social networks is essential to protect user privacy and ensure a safe online environment. A good access control system should be user-friendly, flexible, relationship-aware, and capable of handling high traffic. It must support real-time updates, block abusive behavior, and maintain transparency through audit logs.