Using the given security case pattern for Instant Messaging (IM) software, the placeholder instances are filled with concrete details from the domain information provided:

\*\*Security Case for Instant Messaging (IM) Software:\*\*

- G1: IM software is acceptably secure in digital communication systems

- C1: IM software enables users to exchange information instantly

- C2: Digital communication systems include environments facilitating instant messaging

- C3: "Acceptably secure" means meeting all relevant security requirements to protect user data and interactions

- S1: Argument that IM software assets are under protection

- J1: Protection of IM software assets supports that IM software is acceptably secure

- G2: All identified IM software critical assets are protected

- C4: Critical assets include Registration information, Registration process, User account information, Authentication information, Login process, Chat logs.

- J2: Each asset's security can be argued separately due to their defined roles within the software

- S2: Respective arguments for IM software critical assets

- G3: "Registration information" as software critical asset is protected

- S3: Argument based on the type of asset belonging to "Data Storage"

- C5: Data Storage is part of the internal structure of the software, focusing on maintaining data within secure confines

- J3: Data Storage as a type of asset is recognized under the PEDD classification and its protection is crucial

- G4: "Registration information," a key element of Data Storage, is protected

- G3: "Registration process" as software critical asset is protected

- G3: "User account information" as software critical asset is protected

- G3: "Authentication information" as software critical asset is protected

- G3: "Login process" as software critical asset is protected

- G3: "Chat logs" as software critical asset is protected

This hierarchical tree displays how the structure of the argument emerges from the top-level goal (G1) of assuring that IM software is acceptably secure within a specified system context. The breakdown into further goals (G2 to G4) and their associated strategies (S1 to S3) elaborates on how protection is applied to various identified critical assets, justified by the specific natures and definitions of those assets.