Given the provided security case pattern, we can instantiate a security case for Instant Messaging (IM) software. Here's the hierarchical tree structure for the security case:

```

G1: IM software is acceptably secure in IM system

S1: Argument that software assets are under protection

- C1: Definition and description of IM software

- C2: Definition and description of IM system

- C3: Definition of acceptably secure

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

G2: All identified software critical assets are protected

S2: Respective arguments of software critical assets

- C4: List of IM software critical assets

- J2: Relationship between assets is clear and can be argued separately

G3: Registration information is protected

S3: Argument of the type which the software critical asset belongs to

- C5: List of software critical asset types in PEDD

- J3: Types of software assets are according to PEDD

G4: Registration information, which belongs to Data Storage, is protected

G3: User account information is protected

S3: Argument of the type which the software critical asset belongs to

G4: User account information, which belongs to Data Exchange, is protected

G3: Authentication information is protected

S3: Argument of the type which the software critical asset belongs to

G4: Authentication information, which belongs to Environment Entity, is protected

G3: Chat logs are protected

S3: Argument of the type which the software critical asset belongs to

G4: Chat logs, which belongs to Data Storage, is protected

```

This security case provides a structured argument starting with a high-level goal of ensuring IM software is acceptably secure, supported by a strategy which outlines overall protection of software assets. Each critical asset of the IM software listed has strategies and goals defined to protect each asset and its type, according to the PEDD classification as required. Each node contains additional context information and justifications directly related to the main goals and strategies to support the overall security argument.