Provided below is the hierarchical tree format of a security case for Instant Messaging (IM) software, based on the given security case pattern:

- Goal (G1, Instant Messaging (IM) software is acceptably secure in Instant Messaging system)

- Context (C1, Definition and description of Instant Messaging (IM) software)

- Context (C2, Definition and description of Instant Messaging system)

- Context (C3, Definition of acceptably secure)

- Strategy (S1, Argument that software assets are under protection)

- Justification (J1, Protection of software assets supports that software is acceptably secure)

- Goal (G2, All identified software critical assets are protected)

- Strategy (S2, Respective arguments of software critical assets)

- Context (C4, List of Instant Messaging (IM) software critical assets)

- Justification (J2, Relationship between assets is clear and can be argued separately)

- Goal (G3, IM software critical asset is protected)

- Strategy (S3, Argument of the type which the software critical asset belongs to)

- Context (C5, List of software critical asset types in PEDD)

- Justification (J3, Types of software assets are according to PEDD)

- Goal (G4, IM software critical asset which belongs to (Type 1) is protected)

- Goal (G4, IM software critical asset which belongs to (Type 2) is protected)

- Goal (G4, IM software critical asset which belongs to (Type 3) is protected)

- Goal (G4, IM software critical asset which belongs to (Type 4) is protected)