Using the provided security case pattern, I will instantiate a security case for Instant Messaging (IM) software. The IM software is considered as the system and the domain-specific terminologies and assets are incorporated from the domain information provided.

### Security Case for Instant Messaging (IM) Software:

```

G1: Instant Messaging (IM) software is acceptably secure in an online communication environment.

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

- C2: Definition and description of an online communication environment

- C3: Definition of "acceptably secure" in the context of software security ensuring confidentiality, integrity, and availability

- S1: Argument that software assets are under protection

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

- G2: All identified software critical assets are protected

- C4: List of IM software critical assets: registration information, registration process, user account information, authentication information, login process, chat logs.

- S2: Respective arguments of 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: Process, Environment Entity, Data Exchange, Data Storage.

- J3: Types of software assets are according to PEDD

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

- G3: Registration process is protected

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

- G4: Registration process which belongs to Process 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 Storage 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 Data Exchange is protected

- G3: Login process is protected

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

- G4: Login process which belongs to Process 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

```

Each goal, context, strategy, and justification has been expanded in this structured format to encompass all relevant details and the relationships between them. I substituted placeholders and employed the structure to represent an instant messaging software security assurance case, addressing various critical assets and their protection measures, organized by their respective PEDD types to maintain clarity in argumentation and structure.