Assumptions

- Sessions require unique identifiers (SessionID) as version strings are not unique across platforms.
- Runtime also required a unique identifier so (RuntimeID) is introduced
- Admin have attribute (StaffID) alongside (UserID) to differentiate between regular users and admins.
- Reviews are stored separately from prompts but linked, enabling detailed tracking of administrative actions.
- Affiliations has a many-to-many relationship with users, allowing multiple memberships and group members.
- Applications are tied to specific platforms, with each user limited to one active application.
- Risk Attributes are managed in a single field for simplicity in tracking risky content.
- Payment Information systems include payment tokens and methods for transaction management.
- User Applications are limited to one active application across platforms, requiring approval before session creation.
- Administrators share the PK of (UserID) since all administrators are users.
- Administrators, who are also users, must declare their user accounts to avoid conflicts.
- User Connections are managed with start dates and descriptions, and their status must be tracked.
- A prompt doesn't have uniquely identifiable attributes, so a foreign key SessionID is used with the date/timestamp attribute to make prompts identifiable.
- A status attribute is added to Application entity to be able to track if approved or pending or rejected.