La Logique du Metier Epic_Events

Actions possibles et des restrictions pour chaque département concernant les interactions avec la base de données dans le cadre du projet CRM pour Epic Events, en tenant compte des informations du cahier des charges :

Département Administration :

Actions possibles :

- Créer, modifier, supprimer des comptes utilisateurs, configurer les rôles et permissions.
- Accès complet aux enregistrements pour des raisons administratives et de maintenance.

Restrictions :

- Doit suivre le principe du moindre privilège pour les autres départements.
- Ne doit pas utiliser son plein accès en dehors des besoins administratifs et de maintenance.

Département Gestion

Actions possibles :

- Créer et modifier tous les contrats, filtrer et afficher les événements.
- Modifier des événements pour associer un collaborateur support.
- Accès en lecture aux informations des clients et événements.

Restrictions :

- Ne peut supprimer aucun contrat ni événement
- Ne peut créer, modifier ou supprimer des clients.

Département Commercial

Actions possibles :

- Créer des clients et les associer automatiquement.
- Mettre à jour les informations des clients dont ils sont responsables.
- Modifier les contrats des clients dont ils sont responsables.
- Filtrer et afficher les contrats.
- Créer un événement pour un client après signature d'un contrat.

Restrictions :

- Ne peut pas modifier les contrats qui ne sont pas associés à leurs clients.
- Accès limité en lecture pour les événements et les clients non associés.

Département Support

Actions possibles :

- Filtrer et afficher seulement les événements qui leur sont attribués
- Mettre à jour les informations concernant les événements dont ils ont la charge.

Restrictions :

- Ne peut ni créer ni supprimer d'événements ou de contrats.
- Accès restreint en lecture pour les clients uniquement dans le cadre des événements qui leur sont attribués.

Toutes ces dispositions doivent être implémentées techniquement avec des mécanismes d'authentification, de contrôle d'accès basés sur les rôles (Role-Based Access Control - RBAC), et avec une architecture de sécurité appropriée au sein de l'application CRM.

Détails techniques sur les implémentation potentielle :

Implémentation des Rôles et Permissions

Pour administrer le système de contrôle d'accès basé sur les rôles (RBAC), on peut établir des groupes de permissions pour chaque département. Par exemple :

admin_permissions : Toutes les permissions CRUD (Create, Read, Update, Delete) sur utilisateurs, clients, contrats, et événements.

gestion_permissions : Permissions CRUD sur contrats (sauf suppression), et permissions de mise à jour (Update) sur les événements pour affecter un support.

commercial_permissions : Permissions de création et mise à jour (mais pas de suppression) sur les clients et contrats liés, ainsi que la création d'événements pour leurs clients.

support_permissions : Permissions limitées à la mise à jour des informations d'événements qui leur sont attribués.

Ces permissions seraient alors attribuées aux utilisateurs en fonction de leur rôle dans l'entreprise. Cela se traduit en pratique par des vérifications d’autorisation avant chaque transaction avec la base de données.

Mesures techniques sécuritaires

• Utiliser Django ORM pour éviter les injections SQL en ne permettant pas de requêtes SQL brutes sans validation.
• Utiliser le framework Django pour Python pour développement qui supportent des mécanismes de sécurité intégrés.
• Mise en place de l'authentification par token .
• Stockage des mots de passe utilisateur sous forme de hash en utilisant l’algorithme robuste bcrypt.

Journalisation et Audit

• Configurer les logs pour enregistrer les informations pertinentes sur les actions des utilisateurs : quelle action a été faite, par qui, quand, et sur quel enregistrement.
• Utiliser Sentry pour capturer les erreurs et exceptions en temps réel, permettant une réponse rapide aux problèmes.

Processus de mise en œuvre

1. Définir un modèle de rôles et permissions.
2. Configurer ces rôles et permissions dans le système CRM en utilisant Django ORM.
3. S’assurer que chaque action CRUD est précédée par une vérification de la permission de l’utilisateur connecté.
4. Établir une procédure d’authentification et d'attribution de token/session sécurisée pour contrôler l’accès aux données.
5. Mettre en place les mécanismes de journalisation et d'audit.

Chaque étape nécessite une attention particulière pour s'assurer que la mise en œuvre n'introduit pas de vulnérabilités nouvelles et que l'expérience utilisateur reste fluide tout en préservant l'intégrité et la sécurité des données de la base de données CRM d'Epic Events.