

Charte Hébergement Web

1.1 Règles générales

- Les demandeurs sont responsables de tout contenu publié ou hébergé sur les serveurs de l'université.
- L'université fournit un support technique limité pour l'hébergement Web.
- L'utilisation de l'hébergement Web de l'université est strictement réservée à des fins éducatives et académiques.
- Les demandeurs ne peuvent pas utiliser l'hébergement Web de l'université pour publier ou héberger du contenu illégal, offensant, diffamatoire, discriminatoire, ou qui enfreint les droits d'auteur ou de propriété intellectuelle d'autrui.
- Les demandeurs doivent être prêts à assumer la responsabilité de la gestion de leur espace d'hébergement Web de l'université et doivent s'assurer de faire des sauvegardes régulières à leur espace d'hébergement.
- Le CRSIC / Service Hébergement se réserve le droit de suspendre ou de fermer un espace d'hébergement Web en cas de violation de cette charte ou de toute autre politique ou réglementation de l'université.

1.2 Respect des lois

Le service Hébergement fourni par le CRSIC / Université de Boumerdes ne peut être utilisé que dans le contexte universitaire à savoir Information, éducation, séminaire, colloque, se rattachant au but principal de l'université.

Le demandeur s'engage à respecter l'ensemble de la réglementation applicable à la diffusion d'informations sur Internet. La transmission ou le stockage d'informations ou données en violation avec les lois et règlements en vigueur est interdite, cela inclut sans y être limité, les documents portant atteinte aux droits d'auteurs, les informations qui présenteraient un caractère menaçant, choquant, violent, diffamatoire, xénophobe ou qui seraient contraire à l'ordre public ou aux bonnes mœurs.

1.3 Dommages liés au service Hébergement

Le demandeur est le seul responsable des dommages et préjudices directs ou indirects, immatériels du fait de son utilisation du service d'hébergement et s'engage à faire des backups réguliers de son espace d'hébergement autrement dit son site web et toutes les informations en relations à savoir la base de données

1.4 Identifiant et mot de passe

Chaque utilisateur du service dispose d'un identifiant et d'un accès confidentiel et personnalisé, par conséquent il s'engage à être le seul à les utiliser sous son entière responsabilité. De même, il supporte seul les conséquences de la perte du ou des mots de passe.

En cas de perte ou de vol, l'utilisateur doit dès que possible informer le CRSIC/service Hébergement qui enverra l'annulation immédiate. Les nouveaux éléments d'identification seront transmis à l'utilisateur par courrier.

1.5 Contenu du/des sites internet

Le demandeur est responsable des propos et des contenus figurant sur son espace. En tout état de cause, le demandeur est responsable de la moralité, du respect des lois et règlements notamment en matière de protection des mineurs et du respect de la personne humaine ainsi que de ses données personnelles et les droits des tiers notamment en matière de propriété intellectuelle ainsi que du contenu du site et de l'ensemble des données communiquées.

1.6 Sécurité et confidentialité

- Les demandeurs doivent prendre toutes les mesures de sécurité nécessaires pour protéger leur espace d'hébergement Web de l'université, y compris la création d'un mot de passe fort et la mise à jour régulière des logiciels et des scripts.
- Les demandeurs ne doivent pas partager leur espace d'hébergement Web de l'université avec d'autres personnes.
- Les demandeurs doivent respecter la confidentialité des informations stockées sur les serveurs de l'université, en particulier les données personnelles des étudiants et des membres du personnel.

1.7 Sécurité et prévention des cyberattaques

- Il est strictement interdit d'utiliser le serveur ou l'espace d'Hébergement pour accomplir des attaques par déni de service (« denial of service attacks ») à l'encontre de tout autre site ou service Internet, ou aider à l'accomplissement de telles attaques.
- Les demandeurs doivent prendre des mesures pour prévenir les attaques DDoS, telles que la mise en place de pare-feux, la limitation de la bande passante et la surveillance de l'utilisation des ressources.
- Les demandeurs doivent être conscients des techniques de phishing et prendre des mesures pour protéger les informations d'identification, telles que l'utilisation de l'authentification multifactorielle et l'identification des courriels suspects.
- Les demandeurs doivent éviter de stocker des informations sensibles telles que les numéros de carte de crédit sur les serveurs de l'université et doivent prendre des mesures pour protéger les informations confidentielles stockées sur les serveurs.

L'hébergement Web fourni par l'université est un outil précieux pour les enseignants et les membres du personnel. Nous espérons que cette charte aidera à garantir une utilisation responsable et sécurisée de ce service. En utilisant l'hébergement Web de l'université, vous acceptez les conditions de cette charte.

Lu et Approuvé