Liste de conformité à la Charte CHATONS

Cette liste de conformité est un support pour aider les CHATONS qui se chargent de donner un avis sur une candidature. Cette liste reste optionnelle et ne se substitue pas à l'appréciation des CHATONS. Elle est avant tout là pour aider les candidats et également pour permettre aux CHATONS un gain de temps dans l'appréciation des candidatures.

Légende

! Critères importants pouvant potentiellement être bloquants
i Suggestions

La détermination d'un critère comme étant bloquant ou non est à l'appréciation de chaque membre.

Vérifications préalables

☐ **!** Le site indiqué est en ligne à partir du moment où la candidature est postée.
☐ **!** Dans le cadre du traitement de la candidature, au moins un service est testable et accessible par les membres du collectif. Un accès à un compte "démo" satisfait cette contrainte si les services ne sont pas déjà en accès libre.
☐ **!** La structure indique qu'elle respecte la charte et ne laisse pas penser qu'elle est déjà membre du collectif (elle peut en revanche indiquer qu'elle est candidate).

i Si le portail des services est un sous-domaine (ex.: `services.monchaton.com`) :

- Vérifier le domaine parent (`monchaton.com`) ainsi que `www.monchaton.com`.
- Si les domaines sont utilisés, s'assurer qu'ils ne sont pas en contradiction manifeste avec la Charte.
- Vérifier la présence de pisteurs et la conformité du site à la législation de son pays (mentions légales).
- Si les domaines sont inutilisés, suggérer une redirection (enregistrement DNS `CNAME`) vers le sous-domaine des services.

Publicité / pisteurs / appels tiers

☐ **!** Aucun pisteur tiers n'est présent.
*Ce point est vérifier avec uBlock Origin, Privacy Badger et/ou NoScript en désactivant les protections de Firefox ainsi que d'éventuels PiHole. Les polices et images tierces sont considérées comme des pisteurs potentiel*s.
☐ **!** Si des statistiques sont faites, elles ne nécessitent pas de consentements préalables des utilisatrices et utilisateurs (https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi).
☐ **i** Si le CHATON est contraint de communiquer via un réseau social centralisé ou privé, l'information est accessible par un autre biais.
Ressource utile : https://antipub.org/resistance-a-l-agression-publicitaire-s-infiltre-dans-les-reseaux-sociaux/

Sécurité

☐ ! Les utilisateurs et utilisatrices ont accès aux informations principales concernant la politique de sécurité.
Si vous traitez des données personnelles ce point est obligatoire d'après la RGPD

Test des sites web de la plateforme avec Mozilla Observatory

☐ ! Les sites web du CHATONS et ses **services sont disponibles via HTTPS**.
☐ i Les sites web via HTTP redirigent bien vers HTTPS.
☐ i Les sites web sont notés B ou plus.
Si ce n'est pas le cas, suggérer d'appliquer les recommandations de sécurité pour les services web https://ssl-config.mozilla.org/

Test des serveurs SMTP de la plateforme avec CryptCheck (vérifiable avec `dig MX monchaton.com`)

☐ i Les serveurs mails sont notés D ou plus.
Si ce n'est pas le cas, suggérer d'appliquer les recommandations de sécurité pour le SMTP.

Engagement des adminsys

☐ i Les personnes qui ont des accès administrateurs, bénévoles ou salariées s'engagent sur une charte concernant des points de confidentialité et de prudence.
TODO : comment une personne s'intègre dans le CHATON pour faire des opérations d'adminsys ? Quel compromis sécurité/inclusivité ?

Audit de sécurité avancé (à réaliser avec l'accord du futur CHATONS ?)

☐ i Avancé : Les autres domaines de la plateforme ne semble pas contenir de portes dérobées (instances *adminer* ouvertes), etc.
Le certificat TLS utilisé par le site web de la structure candidate peut éventuellement aider à révéler ces sous-domaines. La liste de publication de Let's Encrypt également.
☐ i Avancé : Il n'y a pas de port critique laissé ouvert par inadvertance.
Pour le vérifier on peut utiliser `nmap`.
☐ i Avancé : Le port SSH a été changé.
☐ i Avancé : Un mécanisme de ban est en place.
Si on fait 10 tentatives de mot de passe erronés quelques part, est-ce qu'on peut continuer ?

Il convient de discuter directement avec les membres de la structure candidate des précautions à prendre (privilégier l'authentification par clefs publiques, forger une bonne passphrase, chiffrement des disques, politique de gestion des accès, etc).

Sauvegardes

☐ ! Les informations relatives aux sauvegardes sont indiquées sur le site web de la structure candidate (et pas seulement dans la candidature).
☐ i La fréquence des sauvegardes, le nombre de copies, l'étendue des sauvegardes, les techniques et les logiciels utilisés sont fiables.
☐ ! Si la politique de sauvegarde présente un ou des risques inhabituels, les utilisateurs et utilisatrices sont correctement informées des limites et des risques.

Fournisseurs et localisation des données

☐ ! Le site indique les lieux d'hébergement des données (y compris des sauvegardes).
☐ ! Le site indique le ou les fournisseurs / sous-traitants du futur CHATONS.
☐ ! Le site indique le degré de contrôle que le CHATON a sur son infrastructure.
Rappel : le CHATON s'engage à afficher publiquement et sans ambiguïté son niveau de contrôle sur le matériel et les logiciels hébergeant les services et les données associées.
☐ ! Le ou les fournisseurs / sous-traitants du futur CHATONS ne sont pas incompatibles avec la charte :

- Vérifier que la juridiction appliquée à l'hébergement de *chaque serveur* de la structure lui permet de respecter la Charte.
- S'assurer, dans la mesure du possible, que la structure n'est pas soumise au Cloud Act et aux autres lois de surveillance américaines.
- **i** Utiliser `whois` sur l'IP et/ou le domaine du site web pour vérifier la localisation de l'infrastructure.
- Les serveurs de la structure sont-ils soumis à la juridiction américaine, ou une autre juridiction que celle de la structure ?
- Les serveurs appartiennent-ils à une société étrangère ? S'ils appartiennent à une société américaine, ils sont soumis au Cloud Act.
- Peut-on localiser chaque serveur utilisé par la structure ?

☐ ! S'ils le sont, l'information est clairement indiquées sur le site du futur CHATON.
Notamment fournisseur de services de paiement en ligne.
☐ ! En cas de location de serveurs (virtuels ou dédiés), le fournisseur s'engage contractuellement à ne pas accéder aux données.

Documentation

Ces informations sont sur le site du futur CHATON, éventuellement dans une rubrique "Documentation".

☐ ! La documentation détaille l'infrastructure globale.

- Niveau de contrôle sur l'infrastructure (accès *root* ?).
- Topologie de l'infrastructure.
- Forme de l'infrastructure (VPS, hébergement web, serveur dédié ?).
- Caractéristiques matérielles (processeur, RAM).
- Système d'exploitation installé sur son ou ses systèmes et sa version, technologies de virtualisation utilisées le cas échéant…
- **i** Liste des paquets installés.

☐ ! La documentation renseigne les procédés nécessaires au déploiement de chaque service.
☐ i Les procédures récurrentes du CHATON sont documentées (éventuellement dans une partie privée).
Exemple : comment faire des sauvegardes, des statistiques, comment créer un compte, un vps à une nouvelle personne…
☐ i Un document ou un paragraphe décrivant les pratiques et mesures de sécurité pour protéger les données et l'infrastructure du futur CHATON existe.
☐ i Un document sur les durées de rétention des logs existe.

Logiciel libre

☐ ! Les services fonctionnent à l'aide de logiciels libres uniquement.
Au sens de la Free Software Foundation, qu'ils soient compatibles ou non avec la licence GPL. Concernant les microcodes matériels pour lesquels il n'y a pas d'alternatives libres fonctionnelles, les logiciels d'amorçages (BIOS), ainsi que tout composant matériel ou logiciel auquel le CHATON n'a pas accès, ce dernier s'engage à en diffuser publiquement la liste, ainsi que leur objet.
☐ ! Sur le site, il y a un lien vers le code source de chaque service.
☐ ! Le CHATON s'engage à n'utiliser que des formats ouverts dans l'exercice de son activité d'hébergement.

CGU & Juridique

Attention : les CGU et les mentions légales sont deux textes distincts.

CGU, CGV, CGS ou règlement intérieur

☐ ! Les **Conditions Générales d'Utilisation / CGU** sont accessibles depuis le site web du futur CHATON.
☐ ! Les CGU sont claires et compréhensibles, à la portée de n'importe qui (pas seulement de juristes).
☐ i Une version courte / condensée est proposée afin de faciliter la compréhension du texte.
☐ ! Les CGU n'excluent pas a priori de potentiels utilisateurs et utilisatrices aux services proposés. Le CHATON peut toutefois définir des « publics cibles » auquel il souhaite s'adresser (par exemple sur des critères de proximité géographique ou autres d'intérêt). Cependant il doit, autant que possible, répondre aux demandes non pertinentes, par exemple en les orientant vers un autre CHATON ou en facilitant l'émergence de structures qui répondraient aux besoins non-satisfaits.
☐ ! Il y a une clause « Données personnelles et respect de la vie privée » indiquant clairement quelle est la politique du CHATON concernant les pratiques visées.
☐ ! Les tarifs de l'ensemble des offres sont décrits publiquement (éventuellement avec un lien ou en renvoyant vers le site).
☐ ! Le futur CHATON s'engage dans ses CGU à ne s'arroger aucun droit de propriété des contenus, données et métadonnées produits par les hébergées ou les utilisateurs et utilisatrices.
☐ ! Les CGU permettent aux utilisateurs et utilisatrices d'obtenir la suppression définitive de toute information (comptes et données personnelles) concernant l'hébergé·e, dans la limite des obligations légales et techniques.
☐ ! Les CGU prévoient la possibilité pour les hébergé·es de quitter les services en récupérant les données associées dans des formats ouverts, dans la mesure du possible.

Mentions légales

Conformément à la loi :
☐ i Les Mentions légales sont accessibles depuis le site web du futur CHATON.
☐ i Les Mentions légales contiennent :
- Le nom du directeur de publication (dans le cas d'une organisation, la dénomination sociale de la personne morale).
- Le nom, prénom, adresse et numéro de téléphone de l'hébergeur.
- Si besoin, des renseignements concernant les droits de propriété intellectuelle (licence des publications) et la politique de stockage des cookies et données personnelles.

Contacts humains

☐ ! Le site permet à toutes les personnes hébergées de communiquer avec le futur CHATON en mettant en avant au moins un moyen de le faire.
Page de contact, numéro de téléphone, mail, liste de diffusion, forum, ticket support, etc. Attention : concernant certains moyens le public doit pouvoir facilement prendre contact.
☐ ! Il est possible de rencontrer physiquement, d'échanger, et de participer au futur CHATON.
☐ ! Les échanges avec les autres CHATONS sont bienveillants.
☐ ! Il n'y a pas de pratique manifestement malveillante envers les utilisateurs et utilisatrices dans les CGU.
☐ i Il n'existe pas de témoignage décrivant un comportement malveillant de la part du futur CHATON.

Accessibilité

Une bonne source de renseignements : https://developer.mozilla.org/fr/docs/Accessibilit%C3%A9

A11y & site du CHATONS

☐ i Le rôle des éléments correspond bien à ce qu'ils représentent visuellement.
Par exemple une balise `<a>` transformée en bouton doit contenir l'attribut `role="button"`. Il faut utiliser les balises titres `<hX>` plutôt qu'agrandir la police d'une `<span>`.
☐ i Les couleurs du site sont suffisamment contrastées afin de ne pas discriminer les personnes malvoyantes.
La mesure du contraste intégrée aux outils de développement de Firefox peut être utile.
*L'outil libre ColorOracle peut aussi être utile.**
☐ i Les images nécessaires pour comprendre la page comportent un texte alternatif avec l'attribut `alt`, les images uniquement décoratives contiennent `alt=""`.
☐ i La page accepte que les utilisateurs et utilisatrices puissent remplacer les styles.
Une feuille de style est utilisée plutôt que des attributs `style=""` permettant de surcharger le style (daltoniens, mal-voyant).
☐ i Suggestion : Lors de l'accès aux services une information sur l'accessibilité du service est donnée.
Il pourrait s'agir d'une icône avec une infobulle.

A11y & services du CHATONS

☐ i Le CHATON fait des Merge Request d'accessibilité sur les services mis en place.

Accessibilité mobile

☐ i Le site est un minimum *responsive* (lisible sur téléphone) sans problème de navigation.

Accessibilité ADSL < 2Mbps

☐ i Les éléments du site web sont suffisamment légers.
Poussé à l'extrême : https://solar.lowtechmagazine.com/fr/2018/09/how-to-build-a-lowtech-website.html.

Apparence, clarté et finition

☐ **i** Si la plateforme vise le grand public, l'apparence générale est suffisante pour qu'elle ne soit pas un frein à l'adoption des services.
☐ **i** Il n'y a pas de liens morts.
☐ **i** La structure a un logo et une identité visuelle qui lui est propre.
☐ **!** Si le service est ouvert sans inscription, le service est accessible via un lien depuis le site web du CHATON.
☐ **!** Si le service est payant ou sur inscription, les modalités d'inscriptions sont claires.
☐ **i** Une page ou un paragraphe décrivant chaque service est présent, avec un éventuel tutoriel afin de guider les utilisateur·ices.

Transmettre à la structure candidate des conseils d'UI/UX pouvant améliorer le design des services et/ou du site.

Annexe : Formulaire de candidature

Aucun champ n'est obligatoire, remplissez ce que vous pouvez :

Nom du futur CHATON :

Nom de la structure parente le cas échéant :
Exemple : le CHATON Chapril pour l'association April, ou Bastet pour Parinux.

Forme juridique de la structure :
particulier, association, entreprise…

Site du futur CHATON : https://

Site de la structure parente le cas échéant : https://

Mentions légales : https://

Conditions Générales d'Utilisation : https://

Journal des incidents et maintenances : https://

Documentation : https://

Détails concernant les sauvegardes : https://
Lien vers les éléments qui expliquent comment les sauvegardes sont faites (contenant : fréquence des sauvegardes, nombre de copies, étendue des sauvegardes, technique et logiciels utilisés).

Liste des requêtes administratives : https://
Précisions sur les requêtes concernant le droit d'auteur : Framablog, Forum.

Rapports d'activité : https://
Ces rapports peuvent inclure une description de votre activité d'hébergement, mais également d'éducation populaire ou d'autres démarches de sensibilisation.

Liste des microcodes propriétaires (le cas échéant) : https://

Lien vers les informations concernant l'hébergement du CHATON :

Exemple de contribution au libre :
Il peut s'agir de merge request, de traductions, de documentations, d'articles, de dons, de souscriptions financières aux éditeurs, d'organisation d'évènements, install party, etc.

Exemple de démarche d'éducation populaire :

Le futur CHATON déclare respecter la charte dans l’entièreté des points requis et déclare notamment :
Il s'agit ici d'une liste des points qui ne peuvent pas être facilement vérifiés par le collectif.

☐détenir les accès administrateur (accès root) sur le système d’exploitation faisant fonctionner les services en ligne finaux ;
☐donner la priorité aux libertés fondamentales de ses utilisateurs et utilisatrices, notamment le respect de leur vie privée, dans chacune de ses actions ;
☐ne faire aucune exploitation commerciale des données ou métadonnées des hébergées ;
☐ne pratiquer aucune surveillance des actions des utilisateurs et utilisatrices, autre qu'à des fins administratives, techniques ou d'améliorations internes des services ;
☐ne pratiquer aucune censure a priori des contenus des hébergées ;
☐ne pas répondre aux requêtes administratives ou d’autorité nécessitant la communication d’informations personnelles avant que ne lui soit présentée une requête légale en bonne et dûe forme ;
☐appliquer ses CGU avec bienveillance ;
☐mettre en œuvre et promouvoir une forme d'organisation et de gouvernance inclusive, capable de s’adapter aux différences et à valoriser la diversité en veillant à ce que les groupes marginalisés ou exclus soient parties prenantes dans les processus de développement ;
☐avoir un modèle économique basé sur la solidarité ;
☐proposer des prix raisonnables et en adéquation avec les coûts de mise en œuvre ;
☐que le salaire (en équivalent temps plein, primes et dividendes compris) le plus faible de la structure ne saurait être inférieur au quart du salaire (en équivalent temps plein, primes et dividendes compris) le plus élevé de la structure.

Précisions éventuelles si le CHATON n'est pas sûr de respecter pleinement la charte :