

Charte d'hébergement de sites Web MCC

V3.0 du 01/01/2011

Table des matières

Article 1 : Objet.....	3
Article 2 : Parties en présence.....	3
Article 3 : Conditions générales.....	3
Article 4 : Responsabilité éditoriale.....	3
Article 4.1 :Condition d'acceptation éditoriale de la création du site.....	3
Article 4.2 : Respect de l'accessibilité.....	4
Article 4.3 : Cas général des contenus.....	4
Article 4.4 : Cas spécifique des contributions externes.....	4
Article 5 : Sécurité du site.....	5
Article 5.1 : Engagements SMOA.....	5
Article 5.2 : Engagements SDSI.....	5
Article 6 : Socle technique SDSI.....	6
Article 7 : Moyens mis à disposition par la SDSI.....	6
Article 7.1 : Moyens spécifiques à chaque site.....	6
Article 7.2 : Moyens mutualisés pour plusieurs sites.....	7
Article 7.3 : Moyens mutualisés dans l'infrastructure SDSI.....	8
Article 8 : Engagement de qualité de service.....	8
Article 9 : Recommandations techniques.....	8
Article 9.1 : Sur la sécurité.....	8
Article 9.2 : Sur le développement des applications.....	9
Article 9.3 : Sur l'accessibilité.....	9

Article 1 : Objet

Différentes entités du ministère ont besoin d'un hébergement de site web dont elles restent maîtres et responsables du contenu. La Sous-Direction des Systèmes d'Information met à leur disposition une capacité d'hébergement sous condition d'acceptation formelle de la présente charte d'hébergement.

Article 2 : Parties en présence

Les personnes physiques ou morales liés par cette charte sont :

- Le Service Maîtrise d'Ouvrage (SMOA) : entité du ministère souhaitant s'engager dans une prestation d'hébergement d'un site web.
- La Sous-Direction des Systèmes d'Information (SDSI) : Sous-direction en charge de la construction et de la production du système d'information du ministère. Son centre technique est au Fort de St-Cyr à Saint-Quentin en Yvelines.
- Le Responsable Opérationnel de la Maîtrise d'Ouvrage (ROMOA) : personne physique désignée par le Service Maîtrise d'Ouvrage pour assurer ses engagements opérationnels.

Article 3 : Conditions générales

L'hébergement d'un site par la SDSI est soumis à certaines conditions :

- ➔ L'acceptation du site par le Département de l'Information et de la Communication (DIC) dans la mesure où il doit s'inscrire dans la politique générale de communication du ministère;
- ➔ La conformité du site aux prescriptions techniques et organisationnelles portées dans cette charte, notamment en terme de respect des spécifications techniques de la SDSI et de respect des règles de maintenance et de sécurité.
- ➔ Toutes les actions à mener par le BSE seront faites en une fois dès la charte signée et les pré-requis fournis par le service demandeur en accord avec les prés-requis de la SDSI.
- ➔ La charte doit être signée avant le lancement d'un marché de réalisation
- ➔ Le planning de réalisation devra être fourni en même temps que la charte.

Cette charte doit être émarginée en double exemplaire par le responsable du SMOA et le responsable de la SDSI. Le responsable SMOA en gardera un exemplaire. L'exemplaire SDSI sera conservé par le Responsable de la Sécurité des Systèmes d'Information de la SDSI pour archivage et une copie sera remise au chef du BSE.

Les coordonnées sont:

Responsable de la Sécurité des Systèmes d'Information
Ministère de la Culture et de la Communication
SG/SDSI
rue du Fort de Saint-Cyr
78182 Saint-Quentin en Yvelines cedex

Article 4 : Responsabilité éditoriale

Article 4.1 : Condition d'acceptation éditoriale de la création du site

Par un courrier aux directeurs d'administrations centrales et régionaux en date du 21 décembre 2004, le directeur de cabinet a décidé que l'ensemble des sites existants devraient être intégrés sur le futur site www.culture.gouv.fr. Cette décision doit être appliquée à tous les contenus existants ou futurs.

De manière générale les domaines « culture.gouv.fr » et « culture.fr » sont sous la responsabilité du DIC qui peut autoriser la création d'un nom de sous domaine spécifique sur la demande d'une direction dès lors que le contenu est lié à un événement ponctuel ou si son hébergement sur les sites www.culture.gouv.fr ou www.culture.fr est techniquement impossible. Dans le cas général, le domaine culture.fr est réservé aux sites à caractère événementiel ou à contenu culturel, et le domaine culture.gouv.fr aux sites de communication institutionnelle.

Le SMOA atteste avoir eu l'autorisation du Département de l'Information et de la Communication (DIC) avant signature de cette charte. La charte devra être accompagnée de l'accord du DIC dans lequel sera précisé explicitement le nom de domaine retenu.

Article 4.2 : Respect de l'accessibilité

Afin de préparer l'application de la loi n° 2005-102 du 11 février 2005 pour « l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées », le SMOA s'engage à assurer l'accessibilité de son site. En particulier il fera prendre en compte les recommandations techniques présentes à la fin de cette charte (article 8.3) pour le développement et la maintenance de son site.

Article 4.3 : Cas général des contenus

Le SMOA reconnaît être informé sur les lois et règlements en vigueur s'appliquant aux personnes morales et physiques diffusant du contenu sur Internet.

Entre autres il reconnaît être informé du fait:

- que les publications constituent notamment des œuvres de l'esprit protégées par les droits d'auteurs au sens de l'article L 112-2 1er et 2° du Code de la Propriété Intellectuelle.
- que les fichiers sons, vidéo ou d'autre nature (MP3, DIVX, ISO, ...) sont soumis aux droits d'auteurs et de propriété intellectuelle.

Le SMOA déclare en conséquence accepter pleinement toutes les obligations légales découlant de la mise en ligne des contenus qui sont présents sur son site.

A ce titre:

- il s'engage à ne pas diffuser sur son site, ni directement ni via un lien hypertexte présent sur le site, des contenus de charme ou à caractère pornographique, raciste ou illégal.
- il assure la SDSI qu'il est titulaire de tous les droits de propriété intellectuelle sur l'intégralité des

pages et données qu'il fait héberger, c'est-à-dire des droits de reproduction, de représentation et de diffusion relatifs au support Internet, pour une durée préalablement déterminée, ou qu'il a obtenu toutes les autorisations nécessaires en matière de droits d'auteur, notamment auprès des sociétés de répartition de droits d'auteur qui seraient requises.

- il instruit les agents qui sont susceptibles de contribuer au contenu du site des règles en vigueur et leur donne des consignes éditoriales claires facilitant leur respect.

La SDSI ne pourra être tenue pour responsable du contenu des informations, du son, du texte, des images, éléments de forme, données accessibles sur les sites hébergés à quelque titre que ce soit.

Article 4.4 : Cas spécifique des contributions externes

Les sites web sont de plus en plus souvent porteurs de dispositifs permettant la contribution d'acteurs externes. Ceux-ci doivent être encadrés pour garantir un contenu du site non seulement conforme à la législation, mais aussi pour préserver l'image du ministère.

Le SMOA s'engage à ne pas diffuser un contenu qui n'aurait pas été préalablement validé par un de ses agents instruits sur les règles en vigueur et ayant reçu les consignes éditoriales adaptées.

A ce titre, le SMOA s'engage à ce que les dispositifs de type forum de discussion, wiki, blog, chat soient modérés a priori (avant publication) par un de ces agents.

Article 5 : Sécurité du site

Article 5.1 : Engagements SMOA

Le SMOA est non seulement responsable du contenu éditorial mais aussi de l'application permettant l'édition, l'administration, la diffusion et toute autre fonction nécessaire aux fonctionnalités de son site, et restant dans le cadre technique autorisé par la présente charte.

Le SMOA s'engage donc à assurer, ou à faire assurer par un prestataire, la maintenance corrective de son site pour effectuer les modifications nécessaires en cas de problème de sécurité ou de dysfonctionnement nuisibles aux ressources mutualisées. A minima, un correctif de sécurité critique devra pouvoir être appliqué dans les 10 jours suivants la demande de la SDSI. Cette maintenance devra aussi garantir le suivi de montée de version du socle technique qui est nécessaire au maintien d'une exploitation cohérente et donc sûre (Article 5). Il est à noter qu'en aucun cas la SDSI n'effectuera d'analyse des causes de dysfonctionnement, ni de maintenance, des applications du site.

Pour faciliter cette maintenance et garantir un niveau de sécurité de base, le SMOA s'engage à n'installer que des versions stables d'applications, et à jour des correctifs de sécurité.

Le SMOA s'engage à désigner et à maintenir à jour la désignation d'un de ses agents au titre de Responsable Opérationnel de son site. Après lecture de la présente charte et acceptation de sa mission, il sera garant du suivi de la sécurité du site et de la mobilisation de la maintenance. Celui-ci sera le correspondant des équipes opérationnelles de la SDSI en cas de problème de sécurité ou lors des montées de version du socle technique. En cas d'absence il devra avoir un remplaçant désigné et connu de la SDSI.

Le ROMOA maintient à jour et communique à la SDSI un document concernant l'architecture (schéma, flux inter composants, ...), l'installation des composants de l'application ainsi que la liste et le contenu des livrables (composants logiciels, briques techniques, dev spécifique, ...) afin que celle-ci soit en mesure d'intervenir sur l'ensemble de l'application si des mesures concernant les problèmes de sécurité étaient à prendre.

D'une manière permanente, le SMOA s'engage à suivre et à mettre en œuvre les mises à jour de sécurité sur l'ensemble des applications de son site. Il en charge officiellement son ROMOA.

Article 5.2 : Engagements SDSI

La SDSI mettant à disposition un socle technique s'engage à mettre en œuvre les correctifs de sécurité sur le système et les applications faisant parties de ce socle. Elle s'engage aussi à faire les montées de versions de ce socle permettant d'échapper à l'obsolescence de certains de ses composants.

La SDSI peut aider le ROMOA à obtenir des informations utiles à la surveillance de la sécurité des applications qu'il utilise en particulier au travers des dispositifs mis en place par la Direction Centrale de la Sécurité des Systèmes d'Information.

La SDSI se réserve le droit d'interrompre le service, notamment si elle juge que ce service constitue un danger pour le maintien de la sécurité, y compris de la disponibilité, de certains moyens de la SDSI, que ce soit suite à un piratage dudit service, ou à la suite d'absence de mise à jour d'application ayant pour conséquence la détection d'une faille dans la sécurité du système. Si le SMOA ne garantit pas au travers du ROMOA un suivi régulier de la sécurité de son site, la SDSI pourra arrêter le service jusqu'à application de ses engagements par le SMOA.

La SDSI s'engage à rétablir le service sur demande du SMOA, dès que les interventions de correction auront été effectuées sous le contrôle du ROMOA, celui-ci en ayant testé et approuvé le résultat.

Article 6 : Socle technique SDSI

La SDSI définit un socle technique mis à disposition sur ses serveurs au-dessus duquel doivent s'installer les applications des sites web.

Au moment de la signature de cette charte le socle technique est construit sur l'ensemble de la distribution Linux CentOS 5.

Pour mémoire celui-ci contient:

- le serveur web Apache en version 2.2,
- l'outil d'administration phpMyAdmin (<http://www.phpmyadmin.net/>) en version 2.11.10
- le serveur de base de données MySQL en version 5.0.77
- l'outil statistique Awstats (<http://awstats.sourceforge.net/>),
- le gestionnaire de liste de diffusion Sympa (<http://www.sympa.org/>) en version 5.4.3
- l'environnement Java 1.6 avec le serveur applicatif tomcat en version 6.0
- l'environnement PHP en version 5.1
- l'environnement Pearl 5.8.8

Ce socle est susceptible d'évoluer pour assurer une exploitation optimale, ne serait-ce que pour prendre en compte les correctifs de sécurité. la SDSI reconnaît toutefois l'importance d'assurer une stabilité de ce socle et ne le changera, sauf cas exceptionnel, que pour suivre les évolutions majeures de version des éléments du socle actuel.

En cas de planification de changement du socle technique, la SDSI informera le SMOA de cette décision. Le SMOA s'engage alors à faire évoluer son application dans les six mois pour être conforme au nouveau socle. En cas d'absence de mise à jour la SDSI pourra arrêter le service jusqu'à

application de ses engagements par le SMOA.

Les sites précédemment installés ne sont pas, pour le moment, soumis à l'utilisation de ce socle, mais pour des raisons de rationalisation de l'exploitation seront progressivement poussés à s'y conformer.

Article 7 : Moyens mis à disposition par la SDSI

Sont mis à disposition du SMOA pour son site web :

Article 7.1 : Moyens spécifiques à chaque site

- Un nom de domaine de la forme “x.y.z.culture.fr” ou “x.y.z.culture.gouv.fr”
La réservation de ce nom de domaine est soumise à l’approbation du DIC. Si par dérogation une autre forme de nom de domaine était acceptée celui-ci serait à la charge du SMOA.
- Un accès FTP pour mettre à jour l'application du site
Cet accès est limité au réseau interne du ministère. Il est confié au ROMOA. Si le site est développé à l’extérieur, le ROMOA peut par exemple réceptionner une livraison au format .ZIP faite par le développeur, et l’installer depuis son poste bureautique du ministère sur le serveur de production de la SDSI.
- Un accès web à des statistiques techniques
L'URL et les moyens d'accès sont confiés au ROMOA. Si le SMOA veut mettre en place des statistiques plus détaillées, il peut utiliser des solutions du marché ne nécessitant pas d'installation spécifique sur le serveur (type Xiti ou GoogleAnalytics) à sa charge.

Article 7.2 : Moyens mutualisés pour plusieurs sites

- De l'espace disque
Bien qu'il n'y ait pas de quotas stricts mis en place, le SMOA doit prévenir la SDSI s'il envisage le dépassement des 100Mo par le site.
- De la bande passante
Bien qu'il n'y ait pas de limitation explicite, le SMOA devra prévenir la SDSI de pointe d'utilisation attendue. Il n'y a pas de garantie particulière de qualité de service réseau.

L'allocation de ressources pour chaque site doit prendre en compte les besoins de l'ensemble des sites hébergés. Son utilisation par chaque site doit donc être raisonnable. A défaut la SDSI pourra en limiter la consommation.

- Un serveur web
- Un serveur applicatifs PHP
La SDSI recommande l'usage de l'environnement PHP/MySQL pour la mise en place de sites dynamiques.
- Un serveur applicatif Java
L'utilisation de l'environnement Java/MySQL n'est pas recommandée par la SDSI mais acceptée, et prévue dans le socle technique. Le serveur applicatif mis à disposition ne permet que l'usage des servlet et jsp. La plate-forme J2EE complète, en particulier le support des EJB, n'est pas disponible. En outre, ce type d'hébergement nécessitant la mise en place d'un reverse-proxy doit être préparé avec attention avec les équipes de la SDSI.
- Un serveur de base de données MySQL et l'outil d'administration associé phpMyAdmin
- Un relais de messagerie électronique
Un relais SMTP est mis à disposition. Il est important de préciser que tout message partant de la

plateforme devra être envoyé par une adresse du domaine « culture.gouv.fr ». ¹Ce relais SMTP bloquera systématiquement tout message adressé à plus de 30 destinataires, et d'une manière générale bloquera tout envoi de mail jugé abusif.

La configuration de ces serveurs mutualisés pour plusieurs sites ne peut être particularisée par site. Les applications installées devront donc être compatibles avec la configuration standard.

Les plate-formes techniques non mentionnées dans la liste ci-dessus (pages ASP, ColdFusion, ...) ne sont pas disponibles dans le cadre de l'hébergement fourni par la SDSI.

Article 7.3 : Moyens mutualisés dans l'infrastructure SDSI

- L'accès et l'usage d'un serveur de liste de diffusion
Pour gérer des listes de diffusion, des lettres d'informations, il faut impérativement utiliser un serveur de liste de diffusion. Un serveur de liste de diffusion est mis à disposition dans l'infrastructure SDSI. Ses modalités d'emploi seront vues au cas par cas entre le ROMOA et les équipes techniques de la SDSI.
- Un relais (proxy) pour les requêtes HTTP vers des serveurs hors du réseau culture
Tout site susceptible d'avoir besoin d'effectuer des requêtes HTTP sortant du réseau culture (récupération de flux rss, interrogation de serveurs de cartographie, etc...) devra obligatoirement passer par le serveur relais (proxy) mis à disposition de façon mutualisée. Ce serveur filtrant sur liste blanche le SMOA devra fournir la liste exhaustive des sites interrogés. Tout autre protocole que HTTP est a priori interdit en sortie du réseau culture.

Article 8 : Engagement de qualité de service

L'organisation de l'équipe d'exploitation est conçue pour fonctionner :

- ➔ de 8h30 à 17h30 du lundi au vendredi
- ➔ et occasionnellement le samedi pour des opérations ponctuelles (journées du patrimoine, fête de la musique,...)

La SDSI garanti le bon fonctionnement du système et des applications du socle technique, ainsi que le maintien d'un accès réseau. En cas d'incident, la SDSI garanti une prise en compte dans les deux heures suivant la signalisation (GTI 2 heures) dans ses plages d'ouverture du service, sans garantir un délais de rétablissement.

Article 9 : Recommandations techniques

Article 9.1 : Sur la sécurité

la SDSI attire l'attention du SMOA sur le fait que les sites dynamiques doivent respecter certaines règles élémentaires en matière de sécurité. En particulier, veiller à respecter les recommandations énoncées dans le document « CERTA-2004-INF-001 » publié par le CERTA :

<http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001/index.html>

¹ Par exemple en [PHP mettre](#) -fexpediteur comme 5ème argument de la fonction mail(). Se référer à la documentation PHP <http://fr2.php.net/manual/fr/ref.mail.php> à ce sujet.

Ces recommandations couvrent les attaques suivantes :

- utilisation des méta-caractères
- failles de codage HTML, PHP, ASP
- attaques de type « SQL injection »

D'une manière générale, quelles que soient les requêtes HTTP envoyées au serveur, celui-ci ne devra pas renvoyer plus d'informations que celles auxquelles le client a droit, ni offrir plus de fonctionnalités.

Par ailleurs afin d'éviter l'afflux de messages indésirables (SPAM), il est recommandé de ne pas mentionner d'adresses de messagerie sous forme textuelles sur les sites publics, y compris dans les données non visibles (méta données, " Dublin core ", références de liens, champs mailto:).

Lorsque l'envoi de messages est nécessaire, il est préférable d'utiliser un formulaire Web permettant au public de contacter l'administration.

Article 9.2 : Sur le développement des applications

La SDSI insiste sur le fait que les serveurs sont sous LINUX, et donc les noms de fichiers et les noms de tables MySQL sont sensibles à la casse. Attention donc aux développements sous Windows, car ce système n'est pas sensible à la casse. Il est recommandé de développer directement sur une plateforme utilisant le même système et les mêmes briques que le socle technique.

Par ailleurs, nos serveurs sont paramétrés avec le charset iso-8859-15, tout site utilisant un autre jeu de caractères, par exemple utf8, doit le gérer explicitement.

Article 9.3 : Sur l'accessibilité

La SDSI insiste sur la nécessité de rendre accessible les sites du ministère, et sur le fait que la prise en compte de ce besoin est plus simple à la conception que lors d'étapes ultérieures de maintenance.

ATTENTION A MODIFIER

En l'attente du RGAA, qui sera la référence réglementaire dès sa publication, les règles techniques retenues par la SDSI sont essentiellement issues du W3C et en particulier des « Web Content Accessibility Guidelines »:

- Le code HTML doit respecter la norme XHTML 1.0 du W3C. Ce code devra passer les tests de validation du W3C. Les feuilles de style (CSS1 ou CSS2) externes seront utilisées pour mettre les feuilles en page. Les feuilles de styles seront validées par le validateur CSS du W3C.
- Les tableaux (Balise <table>) ne seront utilisés que pour la présentation de données et non pour la mise en forme générale des pages. L'utilisation d'images transparentes ou autres astuces similaires de mise en forme sera proscrite. Les unités de positionnement seront relatives. Les frames et les fenêtres pop-up sont interdites. Tout changement de fenêtre principale sera indiqué dans l'attribut "title" du lien dans le cas exceptionnel où ces fenêtres seraient utilisées.
- La page d'accueil doit être validée obligatoirement au niveau AAA selon les Web Content Accessibility Guidelines du W3C. Les pages à fort contenu médias (images, vidéo, son) pourront fonctionner en "mode dégradé" et ne valider que le niveau AA ou A. Pour ces pages, une présentation alternative et accessible sera donnée avec une facilité de mise à jour synchrone. L'accès à ces pages alternatives doit être proposé près du lien menant à la page inaccessible.
- Les pages alternatives contiendront des descriptifs pour les images et graphiques de données, des descriptions audio-orales (type audiovision) pour les vidéos auxquelles mènera un "D Link"

près des images. Les reproductions d'œuvres picturales ou sculpturales seront dotées d'un D-Link où sera proposée une description synthétique de l'œuvre en autant de langues que prévu pour le site "valide". Chaque fois que possible, on prévoira une feuille de style « aural.css » et une feuille de style « braille.css » pour les pages ne satisfaisant pas au niveau AAA.

- Un ordre logique d'accès aux liens sera prévu incluant des « accesskey ». Les liens menant à des pages inaccessibles seront signalés.
- L'usage des technologies ActiveX et Flash MX est interdit.

La SDSI insiste sur le fait que ces règles n'interdisent pas l'utilisation de "javascript" (en feuilles externes exclusivement) mais que son usage doit exclure les purs effets de bluff et d'animation.

Des fiches de conseils pratiques sur l'accessibilité sont disponibles à l'adresse suivante :

<http://www.culture.gouv.fr/cric/accessibilite/niouze.html>

L'accessibilité des pages sera recettée à l'aide du robot Bobby CAST :

<http://bobby.watchfire.com/bobby/html/en/index.jsp>

La qualité du code HTML sera recettée à l'aide du robot du W3C : <http://validator.w3.org/>

La qualité de la CSS, obligatoirement structurée, sera recettée à l'aide du robot du W3C :

<http://jigsaw.w3.org/css-validator/validator-uri.htm>