Échantillon extrait du portfolio de Gwendoline Clavé
Traductrice anglais-français de contrats et supports de communication
Site : www.clavoline-traduction.fr
E-mail : gwen@clavoline-traduction.fr

Confidentiality and Security Agreement

Vendor's Security Obligations

Protection of Client System.

To any extent that in providing the Services Vendor has access to the Client System (which includes, without limitation, Vendor's transmission or storage of electronic files or other electronic data to the Client System), Vendor shall meet all commercially reasonable technological security standards, including, but not limited to, the use of computer firewalls, strong user authentication, encrypted transmissions and storage, anti-malware programs, regular and timely software security patch application, and controlled access to the physical location of computer hardware, to protect the Client Confidential Information and the Client System against any damage, disruption or interference from any destructive computer programming including, but not limited to, harmful computer instructions, viruses, Trojan horses, and worms ("Harmful Code") introduced by or through any hardware or software delivered or used by Vendor.

Secure Internet Transmission.

If Vendor uses the Internet to send or receive Client Confidential Information, then Vendor shall use Internet standard encryption technologies, including, but not limited to, 128-bit Secure Socket Layer (SSL), to provide a secure environment for conducting transactions and transferring Client Confidential Information.

Security Reviews.

Vendor shall conduct periodic reviews, not less frequently than once a year, of any Vendor electronic systems storing Client Confidential Information, in order to evaluate the security risks of such systems. In addition, Client may conduct periodic vulnerability scans of any network or site maintained by or for Vendor that houses Client Confidential Information. Vendor shall take all reasonable steps to facilitate such scans by Client, and shall promptly remediate any material vulnerability identified by Client in the course of such scans.

Accord de confidentialite et de securite

Obligations de securite du Prestataire

Protection du Systeme du client

Dans la mesure où la fourniture des Services permet au Prestataire d'accéder au Système du client (ledit accès comprenant notamment la transmission ou le stockage de fichiers électroniques ou d'autres données électroniques par le Prestataire sur le Système du client), le Prestataire doit satisfaire à l'ensemble des normes de technologies de sécurité commercialement raisonnables, et notamment l'utilisation de pare-feux sur les ordinateurs, l'authentification forte des utilisateurs, le chiffrement des transmissions et du stockage, les programmes anti-malware, l'application fréquente de correctifs de sécurité des logiciels dans les meilleurs délais et le contrôle de l'accès à l'emplacement physique du matériel informatique, afin de protéger les Informations confidentielles du client et le Système du client contre tous dégâts, perturbation ou interférence causés par quelque programme informatique de nature destructrice que ce soit, et notamment les instructions informatiques nuisibles, les virus, les chevaux de Troie et les vers (le « Code nuisible ») introduits par ou au moyen de tout logiciel ou matériel informatique livré ou utilisé par le Prestataire.

Securite des transmissions par Internet

Si le Prestataire utilise Internet pour envoyer ou recevoir des Informations confidentielles du client, le Prestataire devra utiliser des technologies standard de chiffrement sur Internet, et notamment le protocole Secure Socket Layer (SSL) 128 bits, afin d'effectuer des transactions et de transférer les Informations confidentielles du client dans un environnement sécurisé.

Évaluations de la securite

Le Prestataire doit procéder à des évaluations périodiques, au moins une fois par an, des systèmes électroniques du Prestataire sur lequel sont stockées des Informations confidentielles du client, afin d'évaluer les risques de sécurité desdits systèmes. Par ailleurs, le Client peut effectuer des analyses périodiques visant à identifier les vulnérabilités de tout réseau ou site géré par ou pour le Prestataire et hébergeant des Informations confidentielles du client. Le Prestataire doit prendre toutes les mesures nécessaires pour faciliter lesdites analyses effectuées par le Client et devra remédier dans les meilleurs délais à toute vulnérabilité matérielle identifiée par le Client au cours desdites analyses.

Source : Vendor Confidentiality and Security Agreement publié par Stanford PACS Digital Civil Society Lab sur le site Digital Impact Toolkit le 9 novembre 2015 sous licence Creative Commons Attribution 4.0 International.
Traduction par Gwendoline Clavé.