ANNEXE 3 : Mesures techniques et organisationnelles pour assurer la sécurité des données

La présente section présente les principes généraux et moyens mis en œuvre pour assurer au maximum la sécurité des données du système d'information d'Acta Digital Services, au regard de l'état de l'art. Ces règles s'appliquent aux données personnelles et non personnelles.

ACCES AUX DONNEES

Chaque utilisateur dispose d'identifiants personnels de connexion (nom d'utilisateur / mot de passe) afin que tous puissent être tenus pour responsables de leurs actions. L'utilisation d'identités partagées n'est autorisée que là où elles sont appropriées le cas échéant, comme des comptes de formation ou des comptes de service.

Les enregistrements des accès des utilisateurs peuvent être utilisés comme éléments probants dans le cadre d'une enquête sur incident de sécurité.

Les accès sont accordés selon le principe du moindre privilège, ce qui signifie que chaque programme et chaque utilisateur obtiendra seulement les privilèges qui lui sont nécessaires pour effectuer son travail.

Le service informatique est en charge et responsable de la gestion des accès et des restrictions d'accès aux dossiers et fichiers. La gestion des accès à des applications spécifiques et à certaines bases de données peut être déléguée à certains correspondants métiers, ou à des prestataires informatiques, selon les conditions définies contractuellement.

ACCES AUX RESEAUX

Un accès aux réseaux est accordé à tous les employés et sous-traitants, selon les procédures de contrôle d'accès d'Acta Digital Services et le principe du moindre privilège.

Tous les employés et sous-traitants bénéficiant d'un accès distant aux réseaux de l'entreprise sont authentifiés par le mécanisme d'authentification du VPN uniquement.

Les réseaux sont séparés selon les recommandations issues des recherches de sécurité sur les réseaux de l'entreprise. Les administrateurs réseaux regroupent les services et systèmes informatiques et les utilisateurs selon les besoins de cette séparation.

Des contrôles de routage des réseaux sont mis en place pour appliquer la politique de contrôle d'accès.

Le service informatique est en charge et responsable des autorisations relatives aux pare-feux.

ACCES AUX APPLICATIONS ET AUX INFORMATIONS

Tous les employés et sous-traitants d'Acta Digital Services bénéficient d'un accès aux données et aux applications nécessaires à leur fonction professionnelle.

Tous les employés et sous-traitants n'accèdent aux données et systèmes sensibles (données RH, santé, bancaires, paie…) qu'en cas de nécessité professionnelle et avec l'accord de la direction.

Les systèmes sensibles sont physiquement ou logiquement isolés afin d'en restreindre l'accès au personnel autorisé uniquement.

REPORTING

Les incidents hautement prioritaires découverts par ou signalés au service informatique d'Acta Digital Services sont remontés à la Direction. Le service informatique prend dans les meilleurs délais les mesures correctives qui s'imposent.

Le RGPD impose de notifier à la CNIL, dans les 72 heures suivant leur découverte, les violations de données personnelles **présentant un risque pour les droits et libertés des personnes** et, dans certains cas, lorsque le risque est élevé, aux personnes concernées. De plus, en cas de violation des données, Acta Digital Services s'engage à auditer l'incident et la sécurité du système.