

Annexe à la charte de bon usage des systèmes d'information (SI) du Conseil départemental des Alpes de Haute-Provence(CD04) destinée aux agents des organismes partenaires qui doivent utiliser le SI du CD04.

Article 1 : Champs d'application

Les règles et obligations énoncées ci-dessous s'appliquent aux agents des organismes partenaires qui doivent utiliser le SI du CD04.

Ce document a pour objet de définir les règles d'emploi des moyens informatiques et les conditions d'accès au SI pour les agents des organismes partenaires avec lesquels une convention est signée.

Ce document est une annexe de la charte pour le bon usage de l'informatique, des réseaux et des télécoms.

Article 2 : Conditions d'accès

Le droit d'accès aux systèmes informatiques est soumis à autorisation préalable et à l'acceptation formelle des éléments de ce document et de la charte pour le bon usage de l'informatique, des réseaux et des télécoms.

Les agents peuvent accéder au système d'information du département à condition de pouvoir disposer d'un équipement informatique du CD04 (Wyse ou poste lourd). Toute connexion à partir d'un ordinateur extérieur n'est pas autorisée.

L'existence d'une convention de partenariat ou de mise à disposition de locaux, de matériel ou d'accès informatique signée entre l'organisme partenaire et le CD04 est un prérequis. Les demandes d'accès doivent se faire par l'intermédiaire du portail des demandes après avoir complété la demande d'accès proposée ci-dessous et en suivant la procédure suivante:

1 : Les demandes sont initiées par le responsable fonctionnel désigné au niveau du CD04. Les précisions sont apportées sur les services à ouvrir et les niveaux d'accès (formulaire « Demande des accès au SI par le responsable hiérarchique » ci-dessous)

2 : Le responsable du traitement des données doit valider la demande d'accès

3 : Si des accès à des applications métiers sont nécessaires, ils doivent être validés par le Responsable d'Application (RA) et à défaut le responsable fonctionnel désigné.

4 : Le document vu et validé par l'ensemble des personnes concernées ainsi que la convention signée entre l'organisme partenaire et le CD04 devront être mis en pièce jointe de la demande LISA pour mise en place par la DSI. (Enregistrer une demande...Droits et accès.....Demande hors catalogue Droits et accès)

Article 3 : Modalités d'accès

Tous les utilisateurs se voient attribuer un identifiant et un mot de passe qui permettent, selon les niveaux d'accès accordés, de :

- se connecter aux serveurs informatiques du réseau en fonction des droits attachés à chacun ;
- utiliser les ressources informatiques disponibles;
- accéder aux informations et ressources;
- créer, stocker des données.

Cet identifiant et ce mot de passe sont strictement personnels, confidentiels et inaccessibles. Chaque utilisateur est donc responsable de l'usage qui en est fait. L'utilisateur est tenu de prévenir l'administrateur s'il constate un problème quelconque (ouverture d'un incident LISA). L'utilisateur est informé que cet identifiant peut être employé pour permettre une identification/authentification à des outils métiers tiers et donc transmis à des partenaires extérieurs.

L'utilisateur s'engage à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences:

- de masquer sa véritable identité ;
- de s'approprier le mot de passe d'un autre utilisateur ;
- d'accéder à des données ou services auxquels il n'est pas autorisé à accéder.

Tout utilisateur doit quitter un poste de travail en verrouillant sa session (CTRL-ALT-SUP... Verrouiller cet ordinateur). En fin de service le poste doit être éteint.

Article 4 : Emploi des clés USB/supports externes

N'utilisez jamais les clés USB qui peuvent vous avoir été offertes lors de vos déplacements (salons, réunions, voyages...) ou trouvées dans des lieux publics: elles sont susceptibles de contenir des programmes malveillants.

L'utilisateur doit éviter les opérations de copie de données sur des supports amovibles, afin d'éviter la perte de données (ex : vol du support externe, perte d'un ordinateur portable contenant d'importantes quantités d'informations confidentielles...).

Article 5 : Emploi de la messagerie

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées, etc.). Lorsque vous recevez des courriels, prenez les précautions suivantes :

- l'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifiez son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail;
- n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts;
- si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée). Vous pourrez ainsi en vérifier la cohérence;
- ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des

courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing ».

- n'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc. ;
- désactivez l'ouverture automatique des documents téléchargés

Article 6 :

Le responsable fonctionnel doit assurer un suivi des demandes réalisées avec les accès associés et mettre à disposition à la DSI ces informations.

Sans élément sur la durée de mise à disposition des services informatique du Département, cette autorisation d'accès est valable 1 an. Si nécessaire, elle devra être renouvelée 1 mois avant l'échéance.

Article 7 :

Les utilisateurs s'engagent à respecter les règles présentées et à signer le document d'attestation de responsabilité proposé ci-dessous.

Demande d'accès au SI par le responsable fonctionnel

Je soussigné(e)

Responsable fonctionnel de Mr/Mme.....
(Préciser l'organisme origine)

☐ Demande un accès au SI du CD (création d'un compte d'accès) à compter du.....et pour une durée de.....

☐ Demande un accès à la messagerie du CD

☐ Demande un accès à internet

☐ Demande des accès aux outils de production bureautique (Pack office, Acrobat Reader)

☐ Demande la possibilité d'impression (préciser le site)

☐ Demande la mise en place d'un poste téléphonique (préciser le site)

☐ Demande l'accès à des dossiers partagés

- Préciser les dossiers....
- Les droits d'accès associés (lecture, écriture, suppression)

☐ Souhaite accéder à des applications métiers (validation requise du Responsable d'Application)

- Préciser les applications métiers et droits associés