Sécurité adaptée aux entreprises

UCOPIA permet de définir des niveaux de sécurité adaptés aux différentes populations des entreprises : employés, prestataires, collaborateurs, clients… Pour chacune de ces populations, le mode d'authentification peut être personnalisé ainsi que les droits d'accès aux applications/ressources du réseau.

Réponse aux obligations légales

UCOPIA permet à l'organisation d'être en conformité avec l'obligation en vigueur en France et en Europe pour l'hôtel de conserver les données de connexion pendant une durée 12 mois (décret 2006-358) de 6 à 24 mois en Europe (directive 2006/24/CE). *

Confort d'utilisation et simplicité d'utilisation

Un accès Internet à toutes les catégories de population, sans ajouter de travail ni de contrainte d'assistance technique à l'établissement.

L'accès zéro configuration, zéro assistance technique pour les visiteurs

Grâce à UCOPIA, les visiteurs peuvent se connecter avec leur propre PC, et bénéficient du confort d'un accès zéro configuration. L'usage est simple pour le visiteur et ne nécessite pas d'assistance technique.

Contrôle d'accès

Contrôle d'accès par profil dépendant du contexte : les employés et visiteurs n'ont bien sûr pas les mêmes droits. De plus, les applications auxquelles une personne aura accès dépend de son profil : visiteur (collaborateur, client, prestataire, …) ou employé et du contexte : heure, lieu.

Décret 2006-358 du 24 mars 2006 :
Toute organisation proposant un accès à internet doit être en mesure de conserver l'ensemble des informations de sessions (date de connexion et identité de l'utilisateur) et de trafic (sites et pages visités) de façon à être capable de communiquer ces données a posteriori lors d'une enquête judiciaire. Si l'organisation n'est pas en mesure de répondre, le responsable légal s'expose à 75 000 € d'amendes et 5 ans d'emprisonnement.