# CHARTE D'UTILISATION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION - XANADU

**Version :** 1.0

**Date d'application :** À définir

**Périmètre :** Tous sites (Atlantis & Springfield) et télétravail

## 1. Objet de la charte

La présente charte a pour objet de définir les règles d'utilisation, de sécurité et de bon usage des ressources informatiques et numériques mises à disposition des collaborateurs par la société XANADU. Elle vise à protéger l'entreprise contre les risques de sécurité (cyberattaques, fuites de données) et à garantir la continuité de l'activité.

## 2. Champ d'application

Cette charte s'applique à :
L'ensemble des collaborateurs, stagiaires, prestataires et partenaires accédant au Système d'Information (SI) de XANADU.
Tous les équipements informatiques (postes de travail fixes, ordinateurs portables, serveurs, smartphones) et logiciels fournis par l'entreprise.
L'utilisation des ressources depuis les locaux (Atlantis, Springfield) ou en situation de mobilité (Télétravail, déplacements).

## 3. Accès et Authentification

L'accès au système d'information est sécurisé par un identifiant personnel au format « p.nom » associé à un mot de passe. Ces éléments d'authentification sont strictement confidentiels et ne doivent en aucun cas être communiqués à des tiers, y compris aux collègues ou managers. L'utilisateur s'engage à respecter la politique de sécurité en vigueur imposant des mots de passe d'au moins douze caractères combinant majuscules, minuscules, chiffres et caractères spéciaux. Par ailleurs, tout utilisateur est tenu de verrouiller sa session par la combinaison de touches Windows + L dès qu'il s'éloigne de son poste de travail, même pour une courte durée.

## 4. Utilisation du Matériel Informatique

L'intégrité du matériel informatique doit être préservée ; il est donc strictement interdit de démonter, modifier ou déplacer les équipements sans l'accord préalable du Service Informatique. Concernant la partie logicielle, les utilisateurs ne disposant pas des droits d'administration pour des raisons de stabilité et de sécurité, l'installation de programmes personnels ou téléchargés est proscrite et toute demande doit transiter par le support. Enfin, pour prévenir les infections par rançongiciels, la connexion de supports amovibles personnels est bloquée ou strictement encadrée, seuls les périphériques fournis et chiffrés par XANADU étant autorisés.

## 5. Usage d'Internet et de la Messagerie

L'accès à Internet et à la messagerie est fourni à titre professionnel, bien qu'une utilisation personnelle raisonnable soit tolérée tant qu'elle n'affecte ni la productivité ni la sécurité du système d'information. Le système de filtrage de l'entreprise bloque l'accès aux sites illicites, pornographiques, de jeux d'argent ou de téléchargement illégal, et toute tentative de contournement via des proxys ou VPN personnels est interdite. De plus, l'utilisateur doit faire preuve d'une vigilance extrême face aux tentatives de phishing, en s'abstenant d'ouvrir des pièces jointes ou de cliquer sur des liens provenant d'expéditeurs suspects et en signalant immédiatement tout incident.

## 6. Protection des Données et Confidentialité

Afin d'assurer leur sauvegarde, les données professionnelles doivent être impérativement enregistrées sur les serveurs de fichiers réseau, via le lecteur S: pour le service ou H: pour les données personnelles, et non sur le disque local du poste. Il est formellement interdit de stocker des données confidentielles de l'entreprise, telles que des fichiers clients ou RH, sur des services de cloud public non approuvés comme Dropbox ou Google Drive. Chaque utilisateur s'engage également à respecter la confidentialité des données personnelles traitées dans le cadre de ses fonctions, conformément au Règlement Général sur la Protection des Données (RGPD).

## 7. Télétravail et Mobilité

En situation de mobilité ou de télétravail, l'accès aux ressources internes comme l'ERP ou les fichiers partagés doit s'effectuer exclusivement via le VPN sécurisé fourni par XANADU. Il est vivement déconseillé de connecter le matériel professionnel à des réseaux Wi-Fi publics non sécurisés sans activer ce tunnel VPN. L'utilisateur est également responsable de la sécurité physique de son matériel lors de ses déplacements et ne doit jamais laisser son ordinateur sans surveillance dans un lieu public ou un véhicule.

## 8. Surveillance et Droit de Contrôle

Pour garantir la sécurité du réseau et assurer la maintenance technique, XANADU met en œuvre des dispositifs de surveillance incluant la journalisation des connexions et le filtrage Web. L'entreprise se réserve le droit d'accéder aux données et correspondances professionnelles en cas de nécessité de service, dans le respect du cadre légal. Toutefois,

les éléments explicitement identifiés comme « PERSONNEL » ou « PRIVE » ne seront ouverts qu'en présence de l'utilisateur ou après information préalable, sauf en cas d'urgence impérieuse ou de risque grave pour l'entreprise.

## 9. Engagements et Sanctions

Le non-respect des règles énoncées dans la présente charte expose l'utilisateur à des mesures graduées pouvant aller de la restriction ou suspension des accès informatiques à des sanctions disciplinaires telles que l'avertissement, la mise à pied ou le licenciement, conformément au règlement intérieur. De plus, des poursuites pénales et civiles pourront être engagées en cas d'infraction à la loi, notamment pour piratage, vol de données ou téléchargement illégal.

**Lu et approuvé.**

**Nom et Prénom : _____**

**Date : _____ / _____ / _____**

**Signature :**