RÉPUBLIQUE DE CÔTE D'IVOIRE

Union – Discipline - Travail

MINISTÈRE DE LA TRANSITION NUMERIQUE ET DE LA DIGITALISATION (MTND)

AGENCE NATIONALE DU SERVICE UNIVERSEL DES TÉLÉCOMMUNICATIONS/TIC (ANSUT)

	Plateau – Abidjan Côte D'Ivoire
Projet	**Projet de Gouvernance électronique** **Réalisation de l'intranet gouvernemental**
Maîtrise d'ouvrage	**Ministère de la Transition Numérique et de la Digitalisation**
Maître d'œuvre	**Agence Nationale du Service Universel des Télécommunications/Tic**
Objet	**Politique d'hébergement des données dans le cloud**

Juin 2021

Fiche de suivi du changement et validation

Suivi du changement

Date	Auteur	Version	Description du changement
14/06/2021	Hermann KANGA	0.1	Version initiale

Validation

Nom	Version approuvée	Fonction	Date
DJIRE Souley	1.0	Directeur de l' Exploitation	17/06/2021

1. CONTEXTE

Dans le cadre du projet de Gouvernance Electronique (eGOUV), l'Etat de Côte d'Ivoire a signé un contrat de licences Entreprise avec Microsoft. Ce contrat de licences, placé sous la gestion technique de l'ANSUT permet de mettre à la disposition des ministères et institutions les services suivants :

- Un Annuaire Intégré ou carnet d'adresse électronique ;
- Une Messagerie Professionnelle eGOUV ;
- Des Outils de collaboration et de sécurité ;
- Le cloud Public Microsoft Azure couplé au Datacenter eGOUV pour l'hébergement d'applications ;
- Support Microsoft Premier ;
- Etc.

Ce document indique la démarche à suivre afin de pouvoir héberger des applications dans le cloud Public Microsoft.
Cette procédure est destinée principalement aux Directeurs des Systèmes d'Information (DSI) des ministères et institutions de la République de Côte d'Ivoire.

2. QU'OFFRE LE CLOUD PUBLIC MICROSOFT AZURE ?

Le cloud Public Microsoft Azure inclut dans le contrat de licences Etat de Côte d'Ivoire – Microsoft est accessible au https://portal.azure.com via authentification forte avec un Compte Professionnel eGOUV.
Avec des niveaux de services peuvent atteindre 99,99%, soit moins d'une heure d'indisponibilité par an, le cloud Microsoft Azure met à disposition les services ci-dessous :

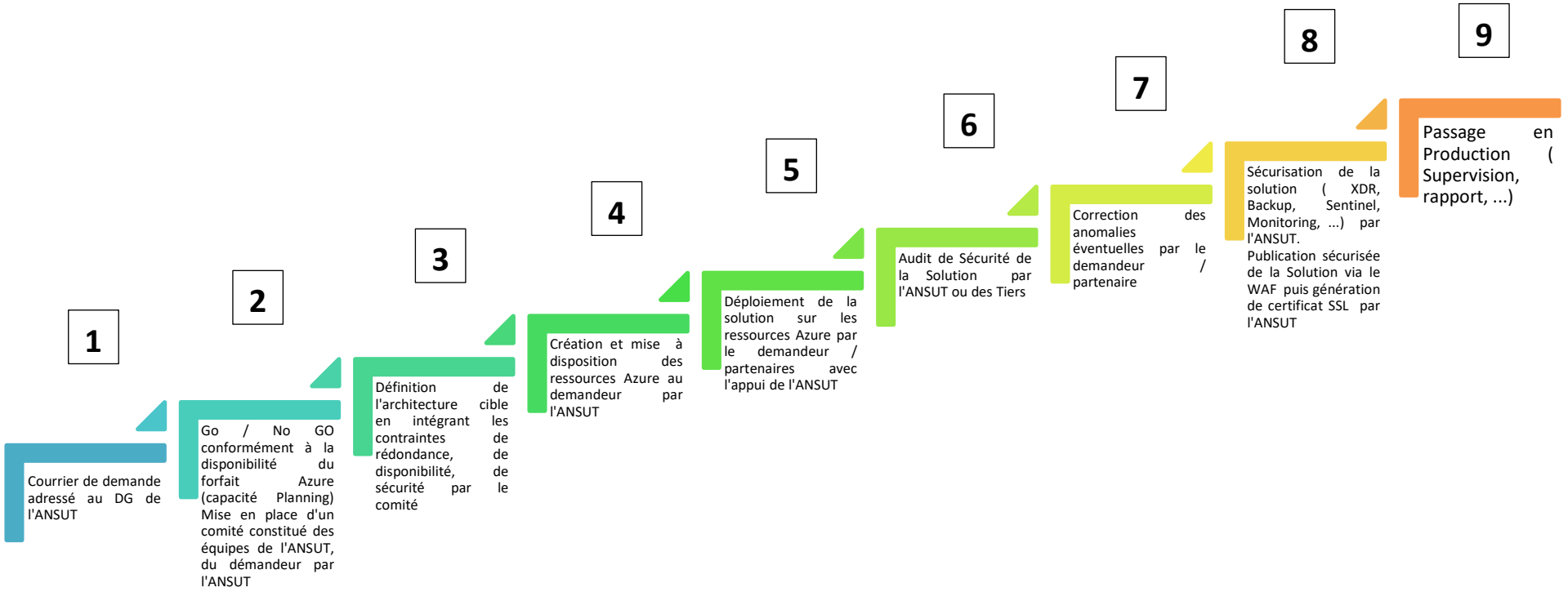
Service Cloud	Description	Exemple
IaaS (Infrastructure as a Service)	Utilisation de machines virtuelles ➔ **Vous hébergez**	VM (1 VC PU, 2 Go de RAM, 150 Go de Disque …)
PaaS (Platform as a Service)	**Vous construisez** à partir d'une base existante de fonctionnalités	Une base de données SQL, PostgreSQL, Microsoft Fabric, IA, …
SaaS (Software as a Service)	**Vous consommez** des services tel quels, vous n'êtes responsables que de vos données.	Office 365, Dynamics 365, Azure Sentinel, …

3. QUI PEUT BENEFICIER DES SERVICES MICROSOFT AZURE ?

Les ministères, les institutions, l'Administration Publique Ivorienne peuvent bénéficier des services fournis par le Cloud Microsoft Azure dans le cadre de leur initiative de transformation digitale.

4. COMMENT BENEFICIER DES SERVICES MICROSOFT AZURE ?

Pour bénéficier des services fournis par le cloud Microsoft Azure, le bénéficiaire à travers son ministre, son Président d'institution ou son Directeur de Cabinet ou le représentant de l'entité administrative adresse un courrier officiel de demande d'hébergement de services dans le cloud Microsoft Azure à Monsieur le Directeur Général de l'ANSUT.



5. ROLE ET RESPONSBAILITE DANS L'EXPLOITATION DES SERVICES HERBERGES DANS LE CLOUD AZURE

L'ANSUT accompagne les bénéficiaires dans l'Exploitation de leur application.
L'ANSUT est responsable de la disponibilité, de la sécurité et de fournir une capacité suffisante pour le bon fonctionnement de la solution. L'ANSUT :

- Vérifie la disponibilité des services et de l'infrastructure ;
- Monitore la sécurité des solutions ;
- Fournit les taux d'usage ;
- Optimise les usages et les coûts ;
- Assiste les bénéficiaires.

Le bénéficiaire est quant à lui responsable du développement de sa solution selon les bonnes pratiques, de son déploiement sur l'infrastructure cloud mise à sa disposition ainsi que du bon fonctionnement de sa solution et de la sécurisation de ses données. Le bénéficiaire est responsable de corriger les anomalies détectées dans sa solution.
L'ANSUT n'a pas accès aux données du bénéficiaire.

6. LES MECANISMES DE SECURITE MIS EN ŒUVRE

Les mécanismes à minima de sécurité des solutions hébergées dans le cloud Microsoft Azure ci-dessous sont mis en place par l'ANSUT :

- **Protection des endpoints :** Tous les endpoints (machines virtuelles, bases de données, stockage) sont protégés par le XDR Microsoft Defender for Endpoint pour une détection en temps réel des menaces.
- **Visibilité centralisée :** le SIEM / SOAR Microsoft Azure Sentinel centralise la collecte et l'analyse des événements de sécurité pour une visibilité complète de l'environnement.
- **Alerte :** Notification par mail en cas de dépassement d'un seuil
- **Sauvegarde robuste :** Les données sont sauvegardées quotidiennement, conformément aux prérequis de la solution par Microsoft Azure Backup pour assurer la récupération en cas de sinistre.
- **Cryptage des données : l**es données sont cryptées lors de leur transit et au repos
- **Contrôle d'accès strict :**
    - **Service Web :** L'accès au service web est strictement contrôlé par un Web Application Firewall (WAF)
    - **Ressources partagées et bases de données :** L'accès est restreint aux adresses IP approuvées, sur demande du demandeur
    - **Accès SSH / RDP :** Les accès SSH / RDP sont restreints par adresses IP, via les services Microsoft JIT Request ou par VPN