Plan d’Assurance de Sécurité

(PAS)

Table des matières

1. Evolutions du document

Date de publication	Auteur
08/09/2021	ORANGE G7

Liste de diffusion

Document diffusé auprès de groupe société INNOV.

2. Introduction

Objet

Le Plan Assurance Sécurité, noté PAS dans la suite de ce document, permet de décrire les engagements pris par ORANGE G7 en termes de sécurité des données et applications lors de la migration des infrastructures de ses clients vers des solutions SDDC.

Périmètre

Le PAS s'applique à tous à tous les services fournis au client, notamment :

- ✓ Les infrastructures
- ✓ Le réseau
- ✓ La sauvegarde
- ✓ Le Plan de Continuité d'Activité (PCA), Le Plan de Reprise d'Activité (PRA)
- ✓ Le Plan d'Assurance de Qualité (PAQ)
- ✓ La fourniture d'un espace de stockage et de partage documentaire
- ✓ L'hébergement de serveurs et d'applications

Les équipes

ORANGE G7 est une équipe technique et commerciale qui est en mission chez les clients pour:

- ✓ Migrer les infrastructures on-premise vers une solution Cloud
- ✓ Virtualiser et optimiser une architecture réseau en une solution full SDN
- ✓ Garantir un niveau de sécurité et un maintien en condition opérationnel
- ✓ Minimiser le cout de fonctionnement

Documents de référence

Les normes :

- ✓ ISO 9001 : Systèmes de Management de la Qualité
- ✓ ISO 27001 : Système de Management de la Sécurité de l'Information (SMSI)
- ✓ ISO 27002 : Code de bonne pratique pour la gestion de la sécurité de l'information

Les règlementations relatives à la Protection des Données Personnelles :

- ✓ Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n° 2018-493 du 20 juin 2018
- ✓ Le Règlement Général sur la Protection des Données (RGPD)

3. Enjeux

Enjeux

La sécurité de la migration des infrastructures, la plateforme d'hébergement et les composants du Système d' Information est une composante essentielle de la protection des intérêts propres du Groupe ORANGE G7, ainsi que celle de ses clients.

Il est donc impératif qu'une Politique de Sécurité du Système d'Information soit mise en œuvre, et qu'elle prenne en compte les principaux risques encourus et identifiés :

- ✓ Risque d'indisponibilité des informations et applications, et des systèmes les traitant.
- ✓ Risque de divulgation, ou perte de confidentialité, accidentelle ou volontaire des informations fournies par notre client et pour lesquelles nous agissons en tant que sous-traitant.
- ✓ Risque d'altération, ou perte d'intégrité, qui pourrait amener à une perte d'information pour nos clients.

Objectifs

Les objectifs de mise en œuvre de la Politique de Sécurité du Système d'Information sont :

- ✓ Améliorer et formaliser la gestion de la sécurité pour les migrations des infrastructures.
- ✓ Prévoir l'extension des services actuels en proposant des services hébergés dans des Cloud publics, par exemple l'offre Azure de Microsoft, qui sont déjà certifiés ISO 27001.
- ✓ Etendre les bonnes pratiques à tous les services proposés par ORANGE G7.
- ✓ S'assurer du respect par ORANGE G7 de ses obligations légales en ce qui concerne la gestion des Données Personnelles (Loi Informatique et Libertés, RGPD), et être en mesure de le démontrer auprès des clients auprès desquels ORANGE G7 intervient

en tant que sous-traitant.

- ✓ Créer une culture de la sécurité auprès des équipes ORANGE G7, et de ses clients.

4. La gestion des risques

La direction générale d'ORANGE G7 souhaite que les risques de sécurité de l'Information qui pourraient conduire à une rupture de services inacceptable pour les clients soient gérés de manière continue. Une analyse des risques a été réalisée selon la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), méthodologie qui est maintenue par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Cette analyse de risques a donné lieu d'une part à la mise à jour de la Politique de Sécurité du Système d'Information (PSSI), et d'autre part à un plan d'actions d'évolution des mesures de sécurité mises en œuvre.

5. Politique de Sécurité du Système d'Information

La mise en application du Règlement Général sur la Protection des Données en mai 2018 a amené de nouvelles obligations imposables aux entreprises et aux sous-traitants.
Afin de répondre à ses obligations réglementaires, d'améliorer ses processus pour y intégrer en permanence l'aspect sécurité de l'information, et ainsi améliorer les pratiques de l'ensemble des équipes techniques, ORANGE G7 met à jour sa Politique de Sécurité du Système d'Information (PSSI).
Cette politique a été mise en place en 2018 et est révisée régulièrement. Elle se base sur les normes de sécurité ISO 27001 et ISO 27002, et est totalement intégrée dans le Système de Management de la Qualité.
La PSSI est diffusée à l'ensemble des personnes concernées, et ORANGE G7 met en œuvre les formations et informations nécessaires à sa compréhension, sa bonne mise en œuvre et son respect.
La PSSI est un document interne à ORANGE G7 et confidentiel. Le Plan Assurance Sécurité (PAS) reprend les informations de la PSSI, communicables aux clients, et selon un plan identique à celui de la norme ISO 27002, pouvant ainsi en faciliter sa lecture et compréhension.

6. Organisation de la sécurité de l'information

Organisation

Chaque salarié possède une fiche de poste qui décrit ses missions, son positionnement au sein de l'organisation d'ORANGE G7, ses principales activités, et les savoir-faire et savoir-être qu'il doit maîtriser pour mener à bien ses missions.

La sécurité est pilotée :

- ✓ Au niveau stratégique au minimum une fois par an lors d'une revue de direction dédiée à la sécurité. Ce comité est composé d'un comité de direction et du RSSI.
- ✓ Au niveau opérationnel lors d'une revue mensuelle. Ce comité est composé du directeur de la BU « Infogérance et Distribution » et de son directeur technique, du directeur du Système d'Information, du RSSI et de l'administrateur ORANGE G7.

Le chef de groupe est le responsable du respect par leurs équipes de la PSSI mise en place.

Veille

ORANGE G7 a qualifié des fournisseurs dans le domaine de la sécurité, et participe régulièrement à des manifestations sur les évolutions dans les domaines réglementaires, techniques, organisationnels et sur les produits.

Gestion des risques dans les projets

La méthodologie projet élaborée par ORANGE G7, dénommée (PE) [2], pour Plan Projet d'Engagement et d'Efficacité, impose la prise en compte de la notion de risques dans tout nouveau projet.

Mobilité et télétravail

L'accès au Système d'Information de ORANGE G7 n'est pas autorisé à des matériels personnels, même au domicile des collaborateurs. Ces accès sont réalisés par l'intermédiaire d'une connexion sécurisée de type VPN.

7. La sécurité des ressources humaines

Embauche

Un projet « arrivé » formalisé permet de structurer l'intégration de tout nouveau collaborateur. Les droits d'accès aux informations et aux applications peuvent évoluer selon le statut de l'intégration (durée minimale de présence, période d'essai terminée, ...).

Confidentialité

Tout collaborateur d'ORANGE G7 a signé une clause de confidentialité dans son contrat de travail.
Tout collaborateur d'ORANGE G7 a pris connaissance de la charte informatique, l'a signée et s'est engagé à la respecter et à la faire respecter.
Cette charte fait également référence aux obligations de confidentialité, et définit les règles de bon usage des ressources informatiques et numériques mises à disposition.

Sensibilisation à la sécurité

Le projet « arrivé » de tout nouveau collaborateur prévoit une sensibilisation à la sécurité, elle est dispensée par le RSSI.
Des sessions de sensibilisation sont organisées de façon annuelle, en présentiel ou sous forme de webinar.

Compétences et formation

La gestion des compétences permet à ORANGE G7 d'identifier les besoins de formation. Les chefs de services définissent les besoins de formation pour leurs équipes, ils sont transmis au service RH pour consolidation et validation d'un plan de formation annuel.

Départ

Un projet « départ » formalisé permet de structurer les actions à mener au départ de tout collaborateur, et en particulier la fermeture de ses comptes d'accès aux différentes ressources auxquelles il avait droit.

8. Gestion des actifs

Inventaire et identification des actifs

Tous les actifs de la plateforme d'hébergement (Azure), ainsi que ceux de tous les collaborateurs ORANGE G7, sont identifiés et inventoriés.

Gestion des supports amovibles

Aucun support amovible n'est utilisé pour la migration des infrastructures vers la plateforme d'hébergement AZURE lors des projets.

Mise au rebus des actifs

Les supports physiques qui contiennent des données sont détruits physiquement avant leur mise au rebus. La seule exception est l'envoi à un constructeur d'un disque dur dans le cadre de la gestion d'un matériel sous garantie, c'est le constructeur dans ce cas qui s'engage à la destruction physique du matériel.

9. Contrôle d'accès

Politique de mot de passe

Chaque utilisateur est identifié par un identifiant unique et un mot de passe fort.
La politique de mot de passe pour les utilisateurs des services hébergés est la suivante :

- ✓ Personnalisation par l'utilisateur lors de sa 1èreconnexion sur l'environnement de production.
- ✓ Taille minimale : 8 caractères
- ✓ Complexité : lettre, chiffre et symbole

- ✓ Fréquence de changement : tous les 4 mois
- ✓ Pas de réutilisation des 5 derniers mots de passe
- ✓ Verrouillage après 5 tentatives infructueuses

Gestion des droits d'accès

La gestion des droits d'accès sur la plateforme d'hébergement Azure se fait à travers Azure Active Directory (AD) qui permet de fournir, en toute sécurité, une authentification unique et une authentification multifacteur pour aider à protéger les clients contre 99,9 % des attaques de cybersécurité.

10. Cryptographie

Transfert de données

Tout transfert de données vers la plateforme d'hébergement est réalisé par l'intermédiaire de liens VPN. Si des données confidentielles doivent transiter soit sur un média amovible, soit dans un mail, ces données doivent être chiffrées en respectant les règles en vigueur.

Chiffrement

Les équipes techniques ORANGE G7 utilisent un logiciel de chiffrement s'appuyant sur l'AES256.

Certificats

Les certificats utilisés par les équipes techniques ORANGE G7 proviennent d'autorités de certifications publiques et reconnues.

Postes nomades

Les disques durs des postes nomades des équipes techniques ORANGE G7 sont chiffrés.

11. Sécurité physique et environnementale

Localisation

Les datacenters sont sités en France.

Sécurité du datacenter

La sécurité de datacenter est garantie pour le fournisseur Microsoft Azure.

Sécurité des matériels

Les matériels et liens d'accès à ceux-ci ont été redondés afin d'éviter toute rupture de service suite à un dysfonctionnement d'un de ces matériels.

- ✓ Redondance du réseau
  - Duplications des routeurs d'accès.
  - Pares-feux en haute disponibilité.
  - Duplication des switchs.
  - Redondance des liens LAN.
- ✓ Redondance des serveurs physiques
  - Redondance des alimentations.
  - Duplication des cartes réseaux.
  - Duplication des cartes fibre optique d'accès au stockage SAN.
- ✓ Redondance du stockage
  - Redondance des switchs optiques.
  - Redondance des contrôleurs SAN.
  - Duplication des chemins d'accès aux SAN.
  - Sécurisation des disques du SAN par des principes de RAID.
  - Disques durs en spare pour pallier les défaillances physiques.
- ✓ Virtualisation
  - Virtualisation des serveurs.
  - Déplacement automatique des serveurs virtuels en cas de défaillance d'un serveur

physique.

12. Sécurité liée à l'exploitation

Procédure d'exploitation

ORANGE G7 est certifié ISO 9001 pour l'ensemble de ses activités, à ce titre les procédures d'exploitation sont documentées, mises à jour et régulièrement auditées.

Logiciels malveillants

Tous les serveurs et postes de travail connectés au Système d'Information ORANGE G7 ainsi que la plateforme d'hébergement utilisée (Azure) sont équipés d'une suite logicielle contre les logiciels malveillants.
La disponibilité de mises à jour est vérifiée quotidiennement, elles sont automatiquement téléchargées et déployés sur les équipements. La supervision et la console centralisée d'administration permettent de détecter immédiatement toute anomalie (mise à jour non déployée, infection, ...)

Sauvegardes

Les données des clients sont sauvegardées tous les jours avec une rétention de 2 semaines.
Les serveurs virtuels des environnements hébergés sont sauvegardés tous les jours avec une rétention de 2 semaines.
Toutes les sauvegardes sont dupliquées dans puisqu'une zone et région sur la plateforme Azure.
Les opérations de sauvegarde sont supervisées, ce qui permet de détecter de suite toute anomalie dans le dispositif.

Tests de restauration

Des tests de restauration sont effectués très régulièrement selon un planning préétabli.

Supervision

Les serveurs, moyens de communication et services sont supervisés en permanence, et des alertes sont positionnées afin que les équipes soient immédiatement informées de toute anomalie potentielle, ou de toute situation pouvant amener à une dégradation du service.

Gestion des mises à jour système

Les mises à jour critiques et de sécurité sont déployées dès leur mise à disposition dès leur validation dans un environnement de tests.

Gestion des mises à jour des applications

Les mises à jour critiques et de sécurité sont déployées dès leur mise à disposition dès leur validation dans un environnement de tests.

13. Sécurité des communications

Architecture technique

Administration et management : un lien dédié est utilisé par les équipes techniques d'ORANGE G7 pour toute intervention sur la plateforme d'hébergement, l'accès à ce lien est filtré aux seules personnes habilitées. En cas de rupture ou d'indisponibilité, l'accès est réalisé en accédant via Internet à des boîtiers SSL qui sont redondés.

Pare-feu

Tous les accès à la plateforme d'hébergement et aux services transitent par des pares-feux ou des boîtiers d'accès SSL.

Détection d'intrusion

Tous les flux d'accès à la plateforme sont analysés afin d'identifier et bloquer les flux anormaux et les programmes malveillants.

14. Acquisition, développement et maintenance des SI

Politique de développement

Les activités de développement sont couvertes par la certification ISO 9001, elles sont décrites et sont conformes aux cycles en V ou aux méthodologies Agile qui sont utilisés par les équipes ORANGE G7.

Toute nouvelle version, que ce soit un correctif, une évolution ou une montée de version a fait l'objet de tests et de validations préalables avant mise en œuvre dans l'environnement de migration. Une phase de retour arrière est prévue si le moindre dysfonctionnement est constaté suite à une mise à jour.

15. Relation avec les fournisseurs

Le fournisseur principal est le Microsoft Azure qui offre une plateforme de cloud reconnu comme l'une des plus grande dans le monde avec plusieurs certifications et caractéristiques permettant d'avoir un niveau de confiance élevé.

Les relations avec ORANGE G7 répondent aux exigences liées au RGPD en prenant en compte l'aspect sécurité.

Toutes les interventions des sous-traitants sont tracées et respectent une procédure, notamment en ce qui concerne les affectations des droits d'accès.

16. Gestion des incidents liés à la sécurité de l'information

Incidents de sécurité

Chaque acteur du SI et de la plateforme d'hébergement, utilisateur ou administrateur, ORANGE G7, Azure, sous-traitant ou Client, est sensibilisé à l'importance de signaler tout incident réel ou suspecté. Ceci inclut le vol de moyens informatiques ou de supports de données. Le signalement des incidents et leur enregistrement sont systématiques. Les Clients le font par l'intermédiaire du Centre de Services ORANGE G7, les utilisateurs internes suivent la procédure mise en place. Cette procédure décrit les escalades et personnes à

alerter selon la gravité de l'incident. Les données statistiques relatives à la gestion des incidents sont intégrées dans le tableau de bord de la sécurité du SI. Un incident de type violation de Données Personnelles respecte les obligations liées au RGPD, il peut faire l'objet d'une notification à la CNIL selon les cas.

Gestion de crise

Le plan de gestion de crise intègre les risques liés à l'informatique ainsi que les risques susceptibles d'une incidence sur le SI ou la plateforme d'hébergement.

17. Gestion de continuité d'activité

Un plan de continuité d'activité est proposé en option aux Clients.

18. Gestion de la conformité

ISO 9001 : ORANGE G7 est certifié ISO 9001 pour l'ensemble de ses activités et de ses sites depuis 2015.
ISO 27001 : les équipes techniques d'ORANGE G7 utilisent les normes ISO 27001 et ISO 27002 pour la gestion de la sécurité pour la fourniture des services auprès de tous les clients.
Données Personnelles : Le Délégué à la Protection des Données Personnelles est le garant du respect par ORANGE G7 de ses obligations.