# Plan Type du PAS

Le Candidat, dans sa réponse, devra impérativement, pour chaque item, élaborer une rédaction détaillée permettant à la CNSA d’analyser la complétude et la qualité des dispositions mises en place par le Candidat en matière de Plan Assurance Sécurité.

Une évaluation du PAS proposé par le Candidat sera réalisée par la RSSI de la CNSA.

|  |
| --- |
| Généralités |
| Préambule |
| Objet du document |
| Documents applicables |
| Documents de référence |
| Termes et définitions |
| Cycle de vie |
| Création |
| Mise en application |
| Vérification |
| Evolution |
| Contexte |
| Rappel du contexte |
| Enjeux |
| Périmètre géographique |
| Périmètre technique |
| Outils utilisés |
| Politiques de sécurité de l’information |
| Orientations de la direction en matière de sécurité de l’information |
| Politiques de sécurité de l’information |
| Revue des politiques de sécurité de l’information |
| Organisation de la sécurité de l’information |
| Organisation interne |
| Fonctions et responsabilités liées à la sécurité de l’information |
| Séparation des tâches |
| Relations avec les autorités |
| Relations avec des groupes de travail spécialisés |
| La sécurité de l’information dans la gestion de projet |
| Appareils mobiles et télétravail |
| Politique en matière d’appareils mobiles |
| Télétravail |
| Sécurité des ressources humaines |
| Avant l’embauche |
| Sélection des candidats |
| Termes et conditions d’embauche |
| Pendant la durée du contrat |
| Responsabilités de la direction |
| Sensibilisation, apprentissage et formation à la sécurité de l’information |
| Processus disciplinaire |
| Rupture, terme ou modification du contrat de travail |
| Achèvement ou modification des responsabilités associées au contrat de travail |
| Gestion des actifs |
| Responsabilités relatives aux actifs |
| Inventaire des actifs |
| Propriété des actifs |
| Utilisation correcte des actifs |
| Restitution des actifs |
| Classification de l’information |
| Classification des informations |
| Marquage des informations |
| Manipulation des actifs |
| Manipulation des supports |
| Gestion des supports amovibles |
| Mise au rebut des supports |
| Transfert physique des supports |
| Contrôle d’accès |
| Exigences métier en matière de contrôle d’accès |
| Politique de contrôle d’accès |
| Accès aux réseaux et aux services réseau |
| Gestion de l’accès utilisateur |
| Enregistrement et désinscription des utilisateurs |
| Distribution des accès aux utilisateurs |
| Gestion des droits d’accès à privilèges |
| Gestion des informations secrètes d’authentification des utilisateurs |
| Revue des droits d’accès utilisateurs |
| Suppression ou adaptation des droits d’accès |
| Responsabilités des utilisateurs |
| Utilisation d’informations secrètes d’authentification |
| Contrôle de l’accès au système et à l’information |
| Restriction d’accès à l’information |
| Sécuriser les procédures de connexion |
| Système de gestion des mots de passe |
| Utilisation de programmes utilitaires à privilèges |
| Contrôle d’accès au code source des programmes |
| Cryptographie |
| Mesures cryptographiques |
| Politique d’utilisation des mesures cryptographiques |
| Gestion des clés |
| Sécurité physique et environnementale |
| Zones sécurisées |
| Périmètre de sécurité physique |
| Contrôle d’accès physique |
| Sécurisation des bureaux, des salles et des équipements |
| Protection contre les menaces extérieures et environnementales |
| Travail dans les zones sécurisées |
| Zones de livraison et de chargement |
| Matériels |
| Emplacement et protection des matériels |
| Services généraux |
| Sécurité du câblage |
| Maintenance des matériels |
| Sortie des actifs |
| Sécurité des matériels et des actifs hors des locaux |
| Mise au rebut ou recyclage sécurisé(e) des matériels |
| Matériels utilisateur laissés sans surveillance |
| Politique du bureau propre et de l’écran verrouillé |
| Sécurité liée à l’exploitation |
| Procédures et responsabilités liées à l’exploitation |
| Procédures d’exploitation documentées |
| Gestion des changements |
| Dimensionnement |
| Séparation des environnements de développement, de test et d’exploitation |
| Protection contre les logiciels malveillants |
| Mesures contre les logiciels malveillants |
| Sauvegarde |
| Sauvegarde des informations |
| Journalisation et surveillance |
| Journalisation des événements |
| Protection de l’information journalisée |
| Journaux administrateur et opérateur |
| Synchronisation des horloges |
| Maîtrise des logiciels en exploitation |
| Installation de logiciels sur des systèmes en exploitation |
| Gestion des vulnérabilités techniques |
| Gestion des vulnérabilités techniques |
| Restrictions liées à l’installation de logiciels |
| Considérations sur l’audit des systèmes d’information |
| Mesures relatives à l’audit des systèmes d’information |
| Sécurité des communications |
| Gestion de la sécurité des réseaux |
| Contrôle des réseaux |
| Sécurité des services de réseau |
| Cloisonnement des réseaux |
| Transfert de l’information |
| Politiques et procédures de transfert de l’information |
| Accords en matière de transfert d’information |
| Messagerie électronique |
| Engagements de confidentialité ou de non-divulgation |
| Acquisition, développement et maintenance des systèmes d’information |
| Exigences de sécurité applicables aux systèmes d’information |
| Analyse et spécification des exigences de sécurité de l’information |
| Sécurisation des services d’application sur les réseaux publics |
| Sécurité des processus de développement et d’assistance technique |
| Procédures de contrôle des changements de système |
| Revue technique des applications après changement apporté à la plateforme d’exploitation |
| Restrictions relatives aux changements apportés aux progiciels |
| Principes d’ingénierie de la sécurité des systèmes |
| Environnement de développement sécurisé |
| Test de conformité du système |
| Données de test |
| Relations avec les fournisseurs |
| Sécurité dans les relations avec les fournisseurs |
| Politique de sécurité de l’information dans les relations avec les fournisseurs |
| La sécurité dans les accords conclus avec les fournisseurs |
| Chaîne d’approvisionnement des produits et des services informatiques |
| Gestion de la prestation du service |
| Surveillance et revue des services des fournisseurs |
| Gestion des changements apportés dans les services des fournisseurs |
| Gestion des incidents liés à la sécurité de l’information |
| Gestion des incidents liés à la sécurité de l’information et améliorations |
| Responsabilités et procédures |
| Signalement des événements liés à la sécurité de l’information |
| Signalement des failles liées à la sécurité de l’information |
| Appréciation des événements liés à la sécurité de l’information et prise de décision |
| Réponse aux incidents liés à la sécurité de l’information |
| Tirer des enseignements des incidents liés à la sécurité de l’information |
| Collecte de preuves |
| Aspects de la sécurité de l’information dans la gestion de la continuité de l’activité |
| Continuité de la sécurité de l’information |
| Organisation de la continuité de la sécurité de l’information |
| Mise en oeuvre de la continuité de la sécurité de l’information |
| Vérifier, revoir et évaluer la continuité de la sécurité de l’information |
| Redondances |
| Disponibilité des moyens de traitement de l’information |
| Conformité |
| Conformité aux obligations légales et réglementaires |
| Identification de la législation et des exigences contractuelles applicables |
| Droits de propriété intellectuelle |
| Protection des enregistrements |
| Protection de la vie privée et protection des données à caractère personnel |
| Réglementation relative aux mesures cryptographiques |
| Revue de la sécurité de l’information |