PRÉSIDENCE
DE LA RÉPUBLIQUE
DU SÉNÉGAL

DCSSI

Politique de Gestion des Actifs

Objectif 6

Les actifs de l'organisme, notamment en matière de système d'information, doivent être identifiés et affectés à des responsables qui doivent en assurer la protection.

REG 1

Procéder à un inventaire précis des actifs de l'organisme afin de les identifier et le mettre à jour

---

REG 2

Affecter les actifs à des responsables désignés et qui sont chargés d'assurer leur sécurité (classification, protection et contrôle d'accès).

REG 3

Identifier, documenter, et mettre en œuvre des règles d'utilisation correcte de l'information, des actifs associés à l'information et des moyens de traitement de l' information.

REG 4

Veiller à la restitution effective des actifs dans leur totalité, en cas de fin de contrat ou de mission.

REG 5

Procéder à une classification des informations suivant leur sensibilité et leur caractère sensible (*cf. Instruction présidentielle no 0303/PR du 16 juillet 2003 mise à jour de l'Instruction présidentielle sur la protection du secret n° 057/PR/SG/DCSSI du 13 janvier 2021).*

REG 6

Les informations stockées dans des supports amovibles doivent être protégées contre toute divulgation, modification ou destruction.

REG 7

Pour les matériels qui doivent être mis au rebut, il faut procéder à un effacement sécurisé des données qui y sont stockées tel que défini par l'Instruction présidentielle no 0303/PR du 16 juillet 2003 (mise à jour de l'Instruction présidentielle sur la protection du secret n° 057/PR/SG/DCSSI du 13 janvier 2021).

PRÉSIDENCE
DE LA RÉPUBLIQUE
DU SÉNÉGAL

DCSSI

Politique de la relation avec les fournisseurs

Objectif 7

Garantir la protection des actifs de l'organisme accessibles aux fournisseurs.

Règle Générale

La sécurité des systèmes d'information de l'organisme englobe tous les aspects, notamment organisationnel, technique, physique et environnemental. A ce titre, tous les intervenants qui ont accès aux systèmes d'information sont concernés par leur sécurité. Ainsi, les prestataires de service, qui sont amenés à intervenir dans les systèmes d'information, doivent se conformer à la politique de sécurité pour assurer la confidentialité, l'intégrité et la disponibilité des données de l'information et des systèmes d'information.

REG 1 Mettre en place une politique de sécurité applicable aux différents fournisseur (logistique, finance, informatique, …)

REG 2 Mettre en œuvre des procédures permettant de surveiller la conformité aux exigences de sécurité de l'information pour chaque fournisseur.

REG 3 Mettre en place un programme de sensibilisation du personnel en contact avec les fournisseurs sur les règles de sécurité applicables à ces derniers ainsi que sur le niveau d'accès aux systèmes d'information.

REG 4 Mettre en place une charte de sécurité signée par les différentes parties qui doivent s'engager à en respecter scrupuleusement les clauses.

REG 5 Rappeler les exigences légales et réglementaires sur les lois relatives à la protection des données à caractère personnel, sur les droits d'auteur et sur la propriété intellectuelle, et veiller à leur respect.

REG 6 Mettre en place un point focal qui sera chargé de communiquer sur les questions de sécurité avec les fournisseurs.

REG 7 Tous les intervenants doivent être pris en compte, notamment les sous-traitants qui travaillent pour le compte de fournisseurs.

REG 8 Les clauses contractuelles entre les fournisseurs et l'entité doivent intégrer toute la chaîne d'approvisionnement informatique : conformité avec les normes relatives à la sécurité des produits informatiques, publication des exigences de sécurité satisfaites par leurs produits et en fournir la preuve.

REG 9 Mettre en œuvre des procédures d'audit sur les prestations effectuées par les fournisseurs ainsi que sur la qualité de ces services