Mesures standards techniques et organisationnelles de sécurité applicables au SMSI de NRB

Organisation de la sécurité générale et du contrôle d'accès

Contrôle clé	Aperçu des mesures techniques et organisationnelles
(référence générale à ISO27K, domaine de contrôles 5.1.x Politiques de sécurité de l'information) : maturité & entretien permanent de celles-ci via le SMSI	• La Politique de sécurité de l'information est en place et contrôlée, et les objectifs de sécurité sont définis en tenant compte de la stratégie commerciale et de l'analyse du risque dans le domaine de la sécurité des informations • La Politique de confidentialité et de Protection des données est en place et contrôlée
(référence générale à ISO27K, domaine de contrôles 6.1.x Organisation de la sécurité de l'information) : organisation et fonctions & responsabilités	• Le responsable de la sécurité est désigné • Un réseau de coordinateurs en sécurité de l'information et de « Relais » est mis en place, des responsabilités sont définies • Un délégué à la protection des données est désigné • (pour la gestion de projets) Les objectifs en matière de sécurité de l'information sont inclus dans les objectifs du projet
(référence générale à ISO27K, domaine de contrôles 8.x) Gestion/Inventaire des actifs	• La politique relative à la classification des données est mise en place et contrôlée • Un inventaire des actifs informatiques est en place, la propriété des actifs est définie • Les actifs informatiques sont classés en fonction de leur criticité (critères dans la politique de classification des données)
(référence générale à ISO27K, domaine de contrôles 18.1.x) Conformité/Contrôle de la conformité	• La politique de conformité est mise en place et contrôlée • (+ implicite dans l'amélioration continue du SMSI, contrôle des autres politiques de sécurité de l'information)
(ISO27K 9.1.x) Politique de contrôle d'accès, Accès aux réseaux et services réseaux	• La politique de contrôle d'accès est mise en place et contrôlée, et couvre l'accès logique et physique des actifs informatiques • L'accès aux actifs informatiques est basé sur les principes du need-to-know/need-to-use (besoin de savoir/besoin d'utiliser) • L'accès au réseau/aux services de réseaux de NRB est soumis à des contrôles techniques et de gestion, afin de garantir que seuls les utilisateurs autorisés peuvent obtenir l'accès (cf. plus bas : gestion de l'utilisateur, mécanismes d'authentification...) • L'utilisation des services de réseaux est contrôlée.
(ISO27K 9.2.x, 9.3.x) Gestion de l'accès utilisateur, Utilisation des informations secrètes	• Enregistrement et désinscription des utilisateurs : le processus pour assigner, autoriser et révoquer les identifiants est défini. L'utilisation d'identifiants partagés n'est autorisée que dans des circonstances

Contrôle clé	Aperçu des mesures techniques et organisationnelles
d'authentification des utilisateurs	exceptionnelles, en cas de nécessité pour des raisons commerciales ou opérationnelles • Distribution des accès utilisateurs : les droits d'accès sont officiellement assignés à des utilisateurs définis sur une base de « need-to-know / need-to-use ». L'accès est modifié/révoqué si les utilisateurs changent de fonction ou quittent l'entreprise. • Les droits d'accès privilégiés sont limités au personnel compétent (par ex. les administrateurs). L'utilisation d'un accès privilégié est soumise à des procédures spécifiques, et l'activité est enregistrée et contrôlée. • Une procédure officielle est mise en place pour envoyer des informations secrètes d'authentification aux utilisateurs (modification obligatoire lors de la première utilisation, exigences minimales pour le mot de passe...). La vérification de l'identité est mise en place pour le cas où les informations d'authentification d'un utilisateur doivent être renouvelées/remplacées • Les utilisateurs reçoivent des consignes relatives à l'utilisation de leurs informations d'authentification (obligation de les garder secrètes/confidentielles, éviter de les enregistrer, interdiction de les partager...) • Les droits d'accès des utilisateurs sont revus à intervalles réguliers, ainsi que lors des changements de fonction. Les droits d'accès sont supprimés ou adaptés au besoin
(ISO27K 9.4.x) Contrôle de l'accès au système et à l'application	• L'accès aux systèmes et applications est limité, conformément aux principes définis dans la politique de contrôle d'accès • Le cas échéant, l'accès aux systèmes et aux applications est soumis à des procédures de connexion sécurisées (procédure d'authentification, protection des mots de passe durant la procédure de connexion, enregistrement et contrôle des tentatives infructueuses, suppression des sessions inactives) • Le système de gestion des mots de passe exige de créer des mots de passe hautement sécurisés (longueur minimale, type de caractères, changement de mot de passe lors de la première connexion, changement de mot de passe à intervalles réguliers, limitation de la réutilisation d'anciens mots de passe...) • Pour les utilisateurs et les programmes utilitaires privilégiés, des exigences de sécurité supplémentaires sont établies, et toutes les activités sont enregistrées et contrôlées (pas uniquement l'activité de connexion). • Le code source des applications et les actifs liés sont strictement limités, et tout accès aux bibliothèques du code source est enregistré et contrôlé

Opérations sécurisées

Contrôle clé	Aperçu des mesures techniques et organisationnelles
(référence générale à ISO27K, domaine de contrôles 11.1.x Zones sécurisées) : périmètre de sécurité physique, contrôles d'accès...)	• La sécurité globale du bâtiment comprend des barrières physiques, un contrôle d'accès avec badge, un système de vidéosurveillance... • L'accès aux « zones sécurisées » identifiées (par ex. le centre de données) est également réservé au personnel autorisé uniquement. Tout visiteur (par ex. le staff technique des fournisseurs) est identifié au préalable (principe de la liste blanche) et reçoit un accès temporaire uniquement
(référence générale à ISO27K, domaine de contrôles 11.2.x Gestion du matériel) : protection, entretien, pratiques d'enlèvement/d'élimination du matériel...	• Le matériel est conservé dans des zones protégées des menaces environnementales (feu, eau, vol...) • Des procédures pour l'enlèvement et l'élimination des actifs informatiques sont établies et contrôlées
(ISO27K 12.1.x) Procédures et responsabilités opérationnelles	• Les procédures opérationnelles sont documentées et accessibles à tous les utilisateurs qui en ont besoin. Les procédures couvrent l'installation/les configurations, la gestion de la sauvegarde et de la récupération, la planification (si applicable), la gestion des erreurs, le contrôle global du système • La gestion officielle des changements est conçue pour gérer les modifications dans l'infrastructure/les procédures/l'organisation d'une manière standardisée (documentation, autorisation, test & approbation finale, mise en œuvre) • Les modifications d'urgence sont soumises à une révision et une approbation explicite • La gestion de la capacité/le contrôle des performances est défini et opérationnel (projections pour des besoins futurs en matière de capacité, suppression des données obsolètes, multiples mesures d'optimisation des performances) • Les environnements de développement, de test et d'exploitation sont séparés. Les procédures de transfert de logiciel entre ces environnements sont établies et contrôlées. • Des mesures de prévention et de détection de logiciels malveillants sont opérationnelles.
(ISO27K 12.3.x) Les principes de sauvegarde, d'archivage et de destruction sont définis et mis en œuvre, et testés régulièrement	• Des procédures de sauvegarde physique sont définies, contrôlées et testées régulièrement • Des procédures de sauvegarde logique et de restauration sont définies, contrôlées et testées régulièrement • Des procédures d'archivage sont définies et contrôlées • Les informations de sauvegarde sont soumises à une protection physique et environnementale

Contrôle clé	Aperçu des mesures techniques et organisationnelles
	• La destruction des sauvegardes et des archives est effectuée comme défini par les procédures
(ISO27K 12.4.x) Journalisation des événements	• La journalisation des événements est établie - globalement & spécifiquement pour les activités de l'administrateur (les journaux globaux enregistrent les événements, les journaux de l'administrateur les détails de l'activité)
(ISO27K 12.5.1) (Système) L'installation du logiciel est soumise à des pratiques standardisées et sécurisées	• Seuls les administrateurs ont l'autorisation et les profils d'accès pour effectuer l'installation ou leurs mises à jour des logiciels du système • Les installations sont soumises à des procédures officielles qui imposent des tests adéquats avant l'installation effective • Une stratégie d'annulation est définie pour toute mise à jour du logiciel du système
(ISO27K 12.6.1) Gestion des vulnérabilités techniques	• Les mesures de prévention et de détection des vulnérabilités techniques sont opérationnelles (à commencer par un inventaire des actifs informatiques et une classification de ceux-ci fondée sur le risque) • Une plage de patching est définie et respectée • Si de nouvelles vulnérabilités sont identifiées, une évaluation des risques est effectuée et des actions définies • Des limitations pour l'installation de logiciels par les utilisateurs sont introduites
(ISO27K 16.1.x) Gestion des incidents	• La politique et les procédures de gestion des incidents sont établies et contrôlées, les rôles & responsabilités sont définis • Le processus de gestion des incidents inclut des principes et conseils relatifs à l'escalade et au reporting, le mécanisme d'évaluation & de réponse, des pratiques « lessons learned » (leçons retenues), des exigences de documentation • Pour des (potentiels) incidents liés à la sécurité et à la vie privée en particulier, des exigences supplémentaires en matière d'escalade et d'analyse sont établies
(ISO27K 10.x) Cryptographie	• Notre politique en matière de cryptographie détermine les cas d'utilisation ainsi que les algorithmes acceptés et les longueurs minimales des clés. Ces recommandations sont en ligne avec les dernières recommandations de la communauté sécurité. • Notre procédure de gestion des clés et certificats est basée sur un workflow avec des R&R clairs pour ce qui concerne la création, la modification et la révocation de ceux-ci. Les données relatives aux certificats sont stockées dans un coffre-fort.

Contrôle clé	Aperçu des mesures techniques et organisationnelles
	• Les données at-rest sur nos baies de stockages et les données en transit sur des réseaux non-gérés par NRB sont chiffrées.
(ISO27K 13.x) Sécurité des communications	• La politique de gestion des réseaux détermine de façon claire les principes à appliquer lors du design et la gestion des réseaux. • Le réseau est divisé en domaines séparés par des éléments de contrôle afin de filtrer de manière adéquate le trafic nord-sud, et d'éviter le trafic est-ouest ; • Les contrôles nécessaires (Dédoublement des systèmes, SSL, VPN, …) sont appliqués afin de préserver la confidentialité, l'intégrité et la disponibilité du réseau et des données • L'accès au réseau est soumis à des règles et contrôles techniques comme le 802.1x • Le réseau de management est dédicacé et est soumis à des exigences et règles d'accès spécifiques.

Développement sécurisé

Contrôle clé	Aperçu des mesures techniques et organisationnelles
(ISO27K 14.1.1) Analyse et spécifications des exigences de sécurité	• Les exigences en matière de sécurité de l'information sont définies pour tout nouveau système/toute nouvelle application d'information que l'on envisage de mettre en œuvre/de développer (y compris par ex. les principes d'authentification et d'accès en fonction de la criticité de l'information, des exigences d'enregistrement, de la formation des futurs utilisateurs...) • Des exigences de sécurité supplémentaires sont définies et mises en œuvre pour tout nouveau système/toute nouvelle application utilisant une infrastructure/des réseaux publics (y compris par ex. des étapes d'authentification, un cryptage, des procédures de confirmation pour l'intégrité des données supplémentaires...) • Des exigences de sécurité supplémentaires sont définies et mises en œuvre pour tout nouveau système/toute nouvelle application impliquant des transactions opérationnelles (y compris par ex. des signatures électroniques, une authentification, des considérations en matière de protection de la vie privée, le cryptage des conversations...)
(ISO27K 14.2.x) Développement sécurisé	• Une politique de développement sécurisé est établie et contrôlée • Une formation de développement sécurisé est dispensée à tous les développeurs couvrant les

Contrôle clé	Aperçu des mesures techniques et organisationnelles
	principes et pratiques de design, de codage et de test sécurisés. • Les environnements de développement, de test et d'exploitation sont séparés. Les procédures de transfert de logiciel entre ces environnements sont établies et contrôlées. • Des procédures officielles de contrôle des modifications sont appliquées pour tout changement de systèmes/ d'applications : des niveaux d'autorité sont définis et respectés, un contrôle des versions est appliqué • Des procédures de test et de conformité sont définies et respectées - à différentes étapes du développement et, à la fin, lors d'un test de conformité par les utilisateurs officiel (y compris un test explicite de sécurité et d'autres exigences « non fonctionnelles ») • En particulier lorsque des plateformes opérationnelles sous-jacentes sont modifiées, toutes les applications critiques utilisant ces plateformes sont également revues et testées • En particulier lorsque NRB fait appel à d'autres fournisseurs pour l'assister dans des activités de développement (externalisation partielle ou complète), des pratiques de développement sécurisé (design, codage, test) sont appliquées contractuellement
(ISO27K 14.3.1) Protection des données de test	• Les environnements de développement, de test et d'exploitation sont séparés. Les procédures de transfert de logiciel entre ces environnements sont établies et contrôlées. • Les données de test sont sélectionnées sur la base des besoins du test - des données opérationnelles ne seront utilisées dans des environnements de test (ou de développement) que dans des circonstances exceptionnelles (ces données opérationnelles seront supprimées une fois que le test est terminé) • Les environnements de test sont soumis à des procédures de contrôle d'accès standard