Organisation visée	Type d'informations		
Groupe Volvo, AA10000	Directive		
Secteur	Numéro du document		Catégorie d'informations
Département de la sécurité, AA14300	0001-27-591		Interne
Responsable	Version	Date de révision	Page
Simonson, Stefan	1.2	11/6/2021	1 / 13

0001-27-591 Normes de contrôle interne Volvo applicables aux TI

Orientation

À l'origine, les Normes de contrôle interne Volvo applicables aux TI (NCIV – TI) étaient réservées aux aspects des TI qui s'avéraient critiques d'un point de vue financier – le tout dans le cadre du Programme de Contrôle Interne du Groupe Volvo. À compter de 2017, la NCIV – TI s'est imposé en tant qu'outil d'analyse d'autres composantes critiques de la structure TI, et à ce titre a été intégrée au Programme de Conformité aux Normes Applicables en Matière de Confidentialité des Données.

Table des Matières

Définitions et acronymes

NCIV-TI : Normes de contrôle interne Volvo applicables aux TI
AFC : Application Financière Critique
SDP : Solution relative aux Données Personnelles
DGS : Directive applicable à la Gestion des Solutions
SGVG : Système de Gestion du Groupe Volvo
GSPC : Gestionnaire des Sous-Portefeuilles Commerciaux
GL : Gestionnaire des Livraisons

Objectif

Les Données de nature Financière et Personnelle sont, par définition, soumis à un encadrement législatif des plus stricts. Tant le Programme de Contrôle Interne que le Programme de Conformité aux Normes Applicables en Matière de Confidentialité des Données du Groupe Volvo ont été conçus en vue d'assurer qu'un tel encadrement est rigoureusement observé chaque fois qu'il s'applique.

Certaines Données de nature Financière et Personnelle sont générées et traitées dans le cadre de différents procédés administrés à l'échelle du Groupe. Or les exigences applicables à de tels procédés sont définies à la Politique de Contrôle Interne ainsi qu'à la Directive Générale Relative aux Données Personnelles – deux (2) énoncés de principes indissociables des activités et transactions commerciales du Groupe.

Dans la mesure où tous les procédés visés sont tributaires d'un environnement TI au sein duquel les informations doivent demeurer disponibles, fiables et à l'abri de toute divulgation non autorisée, un tel environnement fait partie intégrante du Programme de Contrôle Interne et du Programme de Conformité aux Normes Applicables en Matière de Confidentialité des Données du Groupe Volvo.

Le principal objectif de la présente Directive est de définir les exigences de contrôle à l'étude, leur champ d'application et les devoirs et responsabilités des parties prenantes concernées.

Champ et étendue d'application

La présente Directive s'applique à tous les propriétaires de solutions ainsi qu'aux membres du personnel participant au développement, à l'entretien et à l'exploitation des procédés TI dont il sera question plus loin. Elle doit également être prise en compte chaque fois qu'une solution ou un autre service est acquis(e) auprès d'un fournisseur externe. (Veuillez, à ce sujet, consulter le répertoire *SharePoint* « Sécurité Infonuagique »).

La Directive s'applique à tous les aspects de l'environnement TI couverts en vertu du Programme de Contrôle Interne et du Programme de Conformité aux Normes Applicables en Matière de Confidentialité des Données du Groupe Volvo.

Caractéristiques du contrôle des TI

La structure de contrôle des TI définit, d'un point de vue axé sur la conformité, les exigences de contrôle applicables en matière de protection des informations. On y abordera également (et sans s'y limiter) les procédés et objectifs suivants :

- L'identification et l'analyse des aspects de l'environnement TI qui sont directement couverts par des programmes de conformité spécifiques;
- La mise en place et la supervision constante d'exigences de contrôle;
- La surveillance et l'évaluation des efforts déployés en vue de se conformer aux exigences.

Identification et évaluation des composantes TI

Toutes les applications susceptibles d'être intégrées aux composantes structurelles définies au Programme de Contrôle Interne et au Programme de Conformité aux Normes Applicables en Matière de Confidentialité des Données du Groupe Volvo doivent être clairement identifiées et classifiées.

- La définition d'une Application Financière Critique et des niveaux de criticité qui s'y rattachent sera établie par le Département de Contrôle Interne du Groupe, puis consignée à la Ligne Directrice portant sur le Contrôle Interne.
- La définition d'une Solution relative aux Données Personnelles et des niveaux de criticité qui s'y rattachent sera établie par le Bureau de la Vie Privée, puis illustrée au *SharePoint* portant sur le Réseau de Confidentialité des Données du Groupe Volvo.

En vue d'assurer (i) que les raisonnements qui sous-tendent les applications adoptées dans le cadre des programmes de conformité sont uniformes à l'échelle du Groupe, et (ii) que toutes les exigences pertinentes sont adéquatement mises en place, tout changement portant sur la classification :

- d'Applications Financières Critiques doit être approuvé par le Département de Contrôle Interne du Groupe;
- de Solutions relatives aux Données Personnelles doit être approuvé par le Département de la protection des renseignements personnels (dont les fonctions seront déléguées au Représentant à la Protection des Données).

Exigences de Contrôle

La plupart des exigences applicables en matière de protection de l'environnement TI sont définies aux Directives Portant sur la Sécurité des TI, qui elles-mêmes se fondent sur les normes générales reconnues en matière de protection des informations. *Il est crucial que tous les intervenants œuvrant au sein de l'environnement TI se conforment aux Directives qui leur sont applicables.*

Les articles qui suivent (qui d'entrée de jeu reprennent les grandes lignes des Directives Portant sur la Sécurité des TI) définissent, d'un point de vue axé sur la conformité, les exigences de contrôle applicables en matière de protection des informations.

Toute exigence de contrôle doit, par définition, tenir compte de ce qui suit :

- La *valeur* (en termes de sensibilité et d'impact) de l'information visée par l'application (considérant l'objectif poursuivi par cette dernière au sein du procédé pertinent);
- Les *caractéristiques de sécurité de l'information* (confidentialité, intégrité, disponibilité…) qui sont susceptibles d'avoir un impact sur sa valeur (telle qu'elle est définie ci-dessus);
- Les *menaces* posées à la sécurité de l'information (en raison d'une erreur humaine, d'un usage abusif, d'un vol, d'une divulgation non autorisée ou d'une atteinte externe, par exemple)

Structure

Les exigences de contrôle applicables sont regroupées au sein de domaines d'application à l'égard desquels certains objectifs de contrôle sont définis. Il incombera aux responsables de la gestion du procédé TI pertinent, aux propriétaires des produits et/ou des services concernés, et même (le cas échéant) à certains fournisseurs TI externes d'établir la meilleure façon de satisfaire à de tels objectifs de contrôle (qui, par définition, variera en fonction du contexte, de la plate-forme et/ou de l'application à l'étude, de la structure organisationnelle en place, des outils disponibles et d'autres paramètres similaires).

L'Annexe 1 (jointe au présent document) édicte certaines règles applicables à l'interprétation et à la mise en œuvre des objectifs de contrôle.

Domaines d'application

Domaine d'Application	Description
Gestion des Accès	Il est crucial, à ce chapitre, d'assurer qu'aucune information confidentielle n'est divulguée à quiconque n'est pas autorisé à y accéder et de maintenir à un minimum les risques que certaines informations ou fonctionnalités soient modifiées par erreur ou rendues indisponibles. Tout membre du personnel en charge de la gestion des accès sera tenu personnellement responsable de ses actes.
Gestion des Changements	À ce niveau, il est crucial de s'assurer que : - les activités en lien avec le développement de systèmes se déroulent au sein d'un environnement sécuritaire; - seuls des changements dûment testés et approuvés sont introduits au sein de l'environnement de travail; - des exigences de sécurité adéquates accompagnent tout changement introduit au sein de l'environnement de travail. Tous les objectifs ci-dessus doivent être satisfaits en vue d'assurer la confidentialité, la disponibilité et l'intégrité des informations et d'éviter toute perturbation des opérations commerciales.
Gestion de Systèmes	Ce domaine d'application couvre un vaste éventail d'activités de protection, y compris : - documentation des actifs et d'ententes de nature contractuelle

	- prévention, identification et confinement de failles et d'autres vulnérabilités - interventions rapides et efficaces en cas d'incidents
Architecture de Sécurité	Ce domaine d'application couvre un vaste éventail d'activités de protection, y compris : - contrôle constant des données d'identité et des droits d'accès - protection des informations par l'entremise de solutions cryptographiques - protection des infrastructures au sein d'environnements exposés ou fragilisés - détection de fuites d'informations

Devoirs et responsabilités

Les devoirs et responsabilités applicables en matière de contrôle s'imposent à la Communauté TI dans son ensemble.

En sus de tels devoirs et responsabilités, les Départements de la Sécurité et du Contrôle Interne du Groupe et le Bureau de la Vie Privée doivent satisfaire aux obligations spécifiques définies ci-dessous.

Département TI (Nova Bus Inc.)

Tel qu'indiqué à l'énoncé des rôles maintenu à jour au Système de Gestion du Groupe Volvo (SGVG), le département en charge des opérations d'affaire doit s'assurer que :

- les Solutions relatives aux Données Personnelles (SDP) et les Applications Financières Critiques (AFC) sont classifiées adéquatement;
- toutes les SDP et AFC sont conformes aux dispositions de la NCIV-TI.
- les activités en lien avec la conformité sont convenablement soutenues et toutes les dérogations potentielles sont corrigées sans délai.

Nova Bus Inc. doit également veiller à ce que chaque solution de nature critique (SDP ou AFC) demeure en tout temps conforme aux exigences de la NCIV-TI.

Département TI du Groupe

Unités de Livraison de Solutions

Dès qu'il est question de Solutions relatives à des Données Personnelles (SDP), d'Applications Financières Critiques (AFC) ou d'autres solutions de nature critique, les Unités de Livraison de Solutions doivent :

- s'assurer que toutes les exigences découlant des Normes de contrôle interne applicables aux TI (NCIV-TI) ont été incluses aux ententes contractuelles en vigueur;

- confirmer la conformité des exigences de contrôle dont le Groupe des TI est responsable en tant que fournisseur;
- s'assurer que toutes les demandes en lien avec la conformité sont acheminées et que des plans de redressement adéquats sont mis en place et rigoureusement suivis.

Propriétaires de Procédés/Services TI

Parce qu'elles sont de nature obligatoire et incontournable, les exigences découlant de la NCIV-TI doivent être mises en place dès la phase de conception de tout procédé ou service. Or il incombe aux départements de la Gestion des Procédés et de la Gestion des Services de développer des procédés et des services conformes aux dispositions de la NCIV-TI.

Département de la Sécurité du Groupe

Il est de la responsabilité du Département de la Sécurité du Groupe de :

- définir les exigences de contrôle applicables en matière de TI, en collaboration avec le Département de Contrôle Interne du Groupe et le Département de la protection des renseignements personnels;
- mettre en place les exigences requises et en assurer le suivi.

Département de Contrôle Interne du Groupe / Bureau de la Vie Privée

En tant que propriétaires de leurs programmes de conformité respectifs, le Département de Contrôle Interne du Groupe et le Département de la protection des renseignements personnels doivent :

- définir en quoi consistent une SPD et une AFC et circonscrire la portée du Programme de Conformité;
- s'assurer que les applications sont classifiées d'une manière uniforme à l'échelle du Groupe Volvo;
- définir l'ensemble des exigences applicables en matière de conformité;
- définir les méthodes d'évaluation et en circonscrire la portée.

Évaluation de la conformité

C'est en vue d'évaluer la conformité aux dispositions de la présente Directive que l'on procédera chaque année à une revue de l'environnement TI couvert aux termes du Programme de Contrôle Interne et du Programme de Conformité aux Normes Applicables en Matière de Confidentialité des Données.

Responsabilité en matière de conformité

La responsabilité assumée par les membres du personnel en charge d'assurer l'observation des dispositions de la présente Directive est définie ci-haut.

Dérogations

Toute dérogation à l'une ou l'autre des exigences de la NCIV-TI doit obéir à la Procédure de Gestion des Exemptions TI. Veuillez, à ce sujet, consulter la présentation *SharePoint* portant sur les Exemptions TI.

Documentation connexe

Disponibles à même le SGVG :

- Directive de Contrôle Interne (VGMS 0001-27-137)
- Directive de Sécurité Applicable aux TI (VGMS 0001-27-441)
- Sécurité des TI – accès aux systèmes (VGMS 0001-27-443)
- Sécurité des TI – gestion d'actifs tangibles (VGMS 0001-27-444)
- Sécurité des TI – gestion des applications commerciales (VGMS 0001-27-445)
- Sécurité des TI – gestion des réseaux et des communications (VGMS 0001-27-450)
- Sécurité des TI – développement de systèmes (VGMS 0001-27-451)
- Sécurité des TI – gestion de systèmes (VGMS 0001-27-453)
- Sécurité des TI – gestion de la sécurité technique (VGMS 0001-27-454)
- Sécurité des TI – gestion des menaces et des incidents (VGMS 0001-27-455)
- Sécurité des TI – évaluation du rendement (VGMS 0001-27-457)
- Sécurité des TI – évaluation des risques posés à l'intégrité d'informations (VGMS 0001-27-458)
- TI et continuité des opérations (VGMS 0001-27-463)
- Sécurité des TI – gestion des chaînes d'approvisionnement (VGMS 0001-27-570)
- Sécurité des TI – gestion des accès et des données d'identité (VGMS 0001-14-25037)
- BSPM – Description du rôle
- DM – Description du rôle
- SL – Description du rôle

Autres documents :

- *SharePoint* – Sécurité Infonuagique
- *SharePoint* – Procédure d'exemption TI
- Politique du Groupe Volvo Relative à l'Architecture des Infrastructures TI (PVAI)
- *SharePoint* – Réseau de Confidentialité des Données du Groupe Volvo

Historique des Versions

Date	Description du changement

2018-11-12	Première version du texte
2021-01-15	Changement de propriétaire
2021-08-16	Changement de propriétaire, mise à jour des dispositions portant sur les dérogations, mise à jour de l'annexe (description des mesures de contrôle)

Annexe 1 – Exigences de Contrôle

Parce qu'ils sont incontournables d'un point de vue axé sur la conformité, les objectifs de contrôle ci-dessous s'appliquent à toutes les Solutions de Nature Critique. Veuillez cliquer sur le code de contrôle pertinent afin d'avoir accès aux informations détaillées contenues au SGVG.

Gestion des accès

Code de contrôle	Description de la mesure de contrôle	AFC Modéré	AFC Élevé	SDP Modéré	SDP Élevé
AM01	**Séparation des activités de gestion des accès** Les conditions suivantes doivent être satisfaites en vue d'assurer une séparation adéquate des activités de gestion des accès : a) La même personne ne peut à la fois approuver les droits d'accès et les fournir à qui de droit; b) La personne qui tient (au niveau du système-cible) un rôle commercial qui s'étend au-delà de privilèges de lecture ou de consultation ne peut fournir aucun droit d'accès.	X	X	X	X
AM02	**Approbation de droits d'accès** Tous les droits d'accès doivent être approuvés par une personne dûment autorisée. Personne ne peut approuver ses propres droits d'accès.	X	X	X	X
AM04	**Révision et retrait de droits d'accès** Les droits d'accès à des fonctionnalités de systèmes et à des informations de nature critique sont passés en revue sur une base régulière en vue d'assurer qu'ils sont convenablement adaptés aux tâches afférentes à l'emploi. Toute dérogation doit faire l'objet d'une enquête et être résolue à l'intérieur d'un délai raisonnable.	X	X	X	X
AM05	**Définition des règles d'autorisation** Les règles d'autorisation applicables aux applications et aux composantes d'infrastructures de soutien doivent être adéquatement définies et documentées.	X	X	X	X
AM06	**Repérage d'activités de nature critique** Tout intervenant dont le compte permet la réalisation d'activités de nature critique encourt sa responsabilité personnelle.	X	X	X	X
AM07	**Connexion à partir de réseaux non vérifiés** Tout accès à une quelconque application à partir d'une zone non vérifiée doit être assujetti à une procédure	X	X	X	X

	d'inscription administrée par l'entremise d'un service de connexion.				
AM08	**Authentification Multi-Paramètres** Toutes les applications et composantes d'infrastructures de soutien doivent être configurées de manière à ne permettre l'accès qu'à certains utilisateurs privilégiés identifiables au moyen d'un mécanisme d'Authentification Multi-Paramètres (AMP).		X		X

Gestion des Changements / Développement d'Applications

Code de contrôle	Description de la mesure de contrôle	AFC Modéré	AFC Élevé	SDP Modéré	SDP Élevé
AD01	**Séparation logique des environnements TI** L'environnement de production est, sur une base logique, séparé des environnements du développement, des essais et de l'assurance-qualité.	X	X	X	X
AD02	**Protection d'informations à l'extérieur d'environnements de production** Le développement de systèmes et d'autres routines opérationnelles doivent être configurés de manière à ce que les informations privilégiées, confidentielles et/ou de nature sensible qui sont reproduites ou déplacées à l'extérieur de l'environnement de production soient protégées à l'encontre de toute divulgation non autorisée.		X		X
AD05	**Essais de sécurité** Tout système en cours de développement devrait être soumis à des essais de sécurité avant d'être approuvé et intégré à l'environnement de production.	X	X	X	X
CM01	**Séparation des activités de gestion des changements** Les activités de gestion des changements suivantes (qui par définition entrent en conflit) devraient être séparées l'une de l'autre : a) Le développement d'un changement et l'autorisation de l'intégrer à l'environnement de production ne devraient pas être assurés par la même personne. b) Le développement d'un changement et son intégration à l'environnement de production ne devraient pas être assurés par la même personne. c) L'autorisation d'intégrer un changement à l'environnement de production et son	X	X	X	X

	intégration subséquente ne devraient pas être assurés par la même personne.				
CM02	**Approbation de changements** Tout changement affectant une quelconque application, base de données ou composante d'infrastructure doit être approuvé par une personne dûment autorisée avant d'être intégré à l'environnement de production – à moins qu'il ne soit de nature urgente, auquel cas il pourra être mis en œuvre immédiatement sous réserve d'être approuvé au cours des quatre (4) semaines suivantes.	X	X	X	X
CM03	**Approbation de tests** Tout changement affectant une quelconque application, base de données ou composante d'infrastructure doit être passé en revue ou faire l'objet d'essais avant d'être intégré à l'environnement de production – à moins qu'il soit de nature urgente, auquel cas il pourra être mis en œuvre immédiatement sous réserve d'être revu/testé et approuvé à l'intérieur d'un délai raisonnable.	X	X	X	X
CM06	**Périodes de temps critiques** L'opportunité d'apporter des changements aux applications et/ou aux composantes d'infrastructure doit être restreinte et contrôlée au cours de certaines périodes critiques afin d'éviter toute indisponibilité ou corruption d'informations		X		

Architecture de Sécurité

Code de contrôle	Description de la mesure de contrôle	AFC Modéré	AFC Élevé	SDP Modéré	SDP Élevé
SA01	**Gestion des accès (solutions hébergées à l'externe)**. Toute solution hébergée à l'externe et requérant une quelconque authentification doit être confirmée par les services d'identification et de gestion du Groupe Volvo afin d'éviter tout accès non autorisé à des informations de nature sensible.	X	X	X	X
SA02	**Encodage d'informations en cours de transfert** Toute donnée ou information devant être transférée doit tout d'abord être encodée. Elle ne pourra, par la suite, être déplacée qu'au moyen d'une communication encodée.			X	X
SA03	**Détection et surveillance d'accès non autorisés** L'organisation doit être en mesure d'identifier toute menace ou attaque (actuelle ou redoutée) et d'y		X		X

	répondre avant que quelque préjudice sérieux ne lui soit causé.				
SA04	**Fuites d'informations** Il importe de prévenir les fuites d'informations au moyen de mécanismes prévoyant l'enregistrement et la surveillance de données personnelles de nature sensible, le suivi des divulgations et la déclaration de toute faille de sécurité.				X
SA06	**Serveurs se trouvant en des zones vérifiées ou à accès contrôlé** Tout serveur susceptible d'héberger des informations et/ou des Données personnelles sensibles doit être entreposé au sein d'une zone vérifiée ou à accès contrôlé.				X
SA07	**Protection d'applications accessibles au moyen d'un navigateur** Toute application Internet accessible au moyen d'un navigateur doit, en tout temps, être surveillée et protégée à l'encontre d'activités nuisibles et de failles de sécurité. Toute vulnérabilité détectée à ce niveau doit être corrigée à l'intérieur d'un délai raisonnable.	X	X	X	X
SA08	**Encodage d'informations strictement confidentielles au repos** Les données strictement confidentielles au repos (i.e., qui ne se déplacent pas d'un appareil à un autre ou d'un réseau à un autre) doivent être protégées au moyen de techniques d'encodage aptes à prévenir toute forme de divulgation non autorisée.				X

Gestion de Systèmes

Code de contrôle	Description de la mesure de contrôle	AFC Modéré	AFC Élevé	SDP Modéré	SDP Élevé
SM01	**Planification de la continuité TI** Il importe de mettre en place (et de tester périodiquement) un plan de continuité TI couvrant les informations, les applications et les composantes d'infrastructure et ayant pour objectif de réduire l'impact d'éventuelles perturbations sur les opérations commerciales de nature critique.	X	X	X	X
SM02	**Sauvegarde et récupération** Il importe d'adopter certaines routines et stratégies de sauvegarde et de récupération des données qui seront appliquées sur une base régulière en vue d'assurer la disponibilité et l'intégrité des informations.	X	X	X	X
	Surveillance des infrastructures				

SM04	Les composantes d'infrastructure doivent être surveillées afin que l'on puisse y détecter rapidement toute défectuosité de système susceptible de compromettre la disponibilité d'informations de nature critique. Toute routine ou stratégie de surveillance doit comprendre des activités d'enregistrement, d'intervention et de résolution.	X	X	X	X
SM05	**Traitement de lots d'informations automatisé** Il importe de surveiller de près tout traitement de lots d'informations automatisé afin d'en assurer l'achèvement à l'intérieur de délais raisonnables et en conformité avec les objectifs d'affaire du Groupe. Toute routine ou stratégie de traitement doit comprendre des activités d'identification, de détection, d'intervention, de résolution, de documentation et de conservation.	X	X		
SM06	**Configuration des mesures de sécurité** Toute mesure de sécurité doit être conforme aux exigences de configuration applicables et être approuvée par une personne dûment autorisée.	X	X	X	X
SM08	**Application de correctifs (*patches*)** Tout correctif doit être appliqué en temps opportun, peu importe que les vulnérabilités qu'il adresse affectent un système ou un logiciel.	X	X	X	X
SM09	**Registre des actifs exact et à jour** Les solutions et les composantes d'infrastructure auxquelles elles se rattachent doivent être documentées à un registre des actifs centralisé au moyen d'informations précises et à jour.	X	X	X	X
SM10	**Ententes détaillées** Une entente détaillée doit être conclue au sujet des exigences que le département TI du Groupe Volvo doit satisfaire chaque fois que les services d'un fournisseur externe sont retenus. Une telle entente, qui d'entrée de jeu doit contenir une clause de vérification (audit), doit tenir compte du type de solution à l'étude et des résultats de l'Évaluation de l'Impact sur les Affaires.	X	X	X	X
SM11	**Destruction de données** La destruction de toutes données conservées ou jugées inadéquates ou non pertinentes après avoir été passées en revue doit être assurée au moyen d'un effacement physique ou d'une procédure d'anonymisation.			X	X

* * * Fin du document * * *