Final

Code de conduite des administrateurs IS

Version	Version date	Author	Description of modifications	Owner
1.0	01/01/08	Smith Stephen	Creation	Coppens Luc
1.2	15/01/07	Smith Stephen	Updates	Coppens Luc
1.3	08/12/08	Smith Stephen	Document Management compliancy	Coppens Luc
1.4	19/07/11	Coppens Luc	Minor corrections	Coppens Luc

Owner	Approver
Name: Coppens Luc Date: 1/9/2011	Name: Elen Jan Date: 1/9/2011

Contents

1. Introduction

Les **droits d'accès privilégié** permettent à une personne d'effectuer des interventions susceptibles d'avoir un impact sur les systèmes informatiques, la communication en réseau ou les comptes, les fichiers, les données ou les processus des autres utilisateurs. Les droits d'accès privilégié sont généralement accordés aux administrateurs de systèmes ou d'applications, aux administrateurs de réseaux, au personnel de sécurité chargé d'intervenir en cas d'incident ou à tout autre employé nécessitant des privilèges particuliers sur un système ou un réseau informatique dans le cadre de ses fonctions.

Les **personnes avec des droits d'accès privilégié** sont tenues de respecter les droits des utilisateurs, l'intégrité des systèmes et des ressources physiques connexes, ainsi que de se conformer aux règles, lois, réglementations et procédures applicables, tout en prenant les règles appropriées nécessaires pour fournir des services informatiques fiables, sûrs et de haute qualité dans les délais impartis.

Les personnes avec des droits d'accès privilégié ont donc l'*obligation de se tenir informées* des procédures, les pratiques commerciales et les directives opérationnelles relatives aux activités de leur département local. Toutes les règlements relatifs à la sécurité seront publiés sur Blue Box (dans la section IS > Policies & Standards).

La fuite ou l'altération d'informations ou d'installations informatiques peut non seulement porter préjudice aux utilisateurs individuels ou à la productivité de l'entreprise, mais également, dans le cas de la Business Area Energy Benelux & Germany, constituer une menace pour la stabilité de l'approvisionnement énergétique globale.

Les personnes avec des droits d'accès privilégié doivent dès lors être *dignes de confiance et maintenir des niveaux élevés d'éthique et de professionnalisme* dans l'exercice de leurs fonctions.

2. Dispositions générales

1. Les droits d'accès privilégié sont uniquement accordés aux personnes autorisées, après validation de leur demande.
2. Les droits d'accès privilégié ne peuvent être utilisés que dans l'exercice des fonctions attribuées par le supérieur hiérarchique désigné ou le responsable de l'IS Energy Benelux & Germany.
3. Si une action peut être effectuée selon des méthodes n'exigeant pas des droits d'accès privilégié, ces autres méthodes doivent être utilisées, à moins que les contraintes liées au délai ou aux autres ressources requises ne justifient clairement l'utilisation de l'Accès privilégié. En cas de doute, il convient de demander l'avis de l'Information Security Manager local avant de prendre une quelconque mesure.
4. Les droits d'accès privilégié ne peuvent être utilisé pour accorder, modifier ou refuser des ressources, un accès ou un privilège à une autre personne que s'il s'agit d'activités autorisées de gestion des comptes ou dans des situations exceptionnelles. Ces interventions doivent strictement respecter toutes les directives et procédures organisationnelles existantes.
5. Dans tous les cas, l'accès aux informations électroniques d'autres personnes (informations sur les comptes de courrier électronique, détails des messages, etc.) sera limité à la durée minimale d'intervention nécessaire pour résoudre une situation et procéder à une lecture attentive du contenu.
6. Les personnes avec des droits d'accès privilégié prendront les précautions techniques (p. ex. verrouillages physiques et technologiques et mesures de sécurité) et organisationnelles (p. ex. procédures de classement et de reporting) pour protéger la confidentialité des informations rencontrées dans l'exercice de leurs fonctions.

   Si, dans l'exercice de leurs fonctions, les personnes avec des droits d'accès privilégié découvrent,

par inadvertance, des informations indiquant éventuellement une utilisation inappropriée de la Technologie de l'Information (comme un accès non autorisé, des tentatives de piratage informatique), elles sont tenues de consulter immédiatement leur Information Security Manager local. Si la situation constitue une menace immédiate pour l'Information Security de la Business Area Energy Benelux & Germany, une intervention peut s'avérer nécessaire sans consultation préalable de l'Information Security Manager local. Dans ce cas, la personne avec Accès privilégié doit informer, dans les meilleurs délais, l'Information Security Manager local de la menace et des mesures prises.

7. Les personnes avec des droits d'accès privilégié doivent constamment actualiser et améliorer leurs connaissances techniques et autres compétences liées à leurs fonctions, et échanger leurs connaissances et expériences entre eux.

3. Preuve de confiance

Les administrateurs qui ne respectent pas les règles de l'IS Energy Benelux & Germany, perdront la totalité de leurs droits d'accès privilégié.