Final

Code of conduct for IS administrators

Version	Version date	Author	Description of modifications	Owner
1.0	01/10/06	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

Privileged access rights enable an individual to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access rights are typically granted to system or application administrators, network administrators, security staff involved in incident response, or other such employees whose job duties require special privileges over a computing system or network.

Individuals with privileged access rights must respect the rights of the users, respect the integrity of the systems and related physical resources, and must comply with applicable policies, laws, regulations, and procedures, while pursuing appropriate actions required to provide high-quality, timely, reliable and secure computing services.

Individuals with privileged access rights have therefore an *obligation to keep up to date at all times* regarding related procedures, business practices, and operational guidelines pertaining to the activities of their local department. All new security policies will be published on Blue Box (in the IS > Policies & Standards section).

Leakage of, or tampering with information or computer facilities may not only adversely impact individual users, or business productivity, but in the case of Business Area Energy Benelux & Germany it might also become a threat to the critical energy infrastructure.

Individuals with privileged access rights must therefore be *trustworthy and maintain a high ethical standard and degree of professionalism* in the performance of all their duties.

2. General Provisions

1. Privileged access rights are granted, following a validated request, only to authorized individuals.
2. Privileged access rights may be used only to perform job duties assigned by their designated hierarchical manager or IS Energy Benelux & Germany responsible.
3. If methods other than using privileged access rights will accomplish an action, those other methods must be used, unless the burden of time or other resources required clearly justifies using privileged access rights. In case of any doubt, the advice of the local Information Security Manager should be sought prior to taking any action.
4. Privileged access rights may be used to grant, change, or deny resources, access, or privilege to another individual only for authorized account management activities or under exceptional circumstances. Such actions must strictly follow any existing organizational guidelines and procedures.
5. In all cases, access to other individuals' electronic information (email account information, message details, internet logs, etc.) shall be limited to the least action necessary to resolve a situation and the least perusal of contents.
6. Individuals with privileged access rights shall take necessary technical (e.g. physical and technological locks and security measures) and organizational (e.g. filing and reporting procedures) precautions to protect the confidentiality of information encountered in the performance of their duties.

   If, during the performance of their duties, individuals with privileged access rights inadvertently see information possibly indicating inappropriate use of Information Technology (such as unauthorized access, hacking attempts) they will immediately consult with their local Information Security Manager. If the situation is an immediate threat to Business Area Benelux & Germany's Information Security, intervening action may be required without prior consultation of the local Information Security Manager. In that case, the

individual with privileged access rights must notify the local Information Security Manager as soon as possible of the threat and the actions taken.

7. Individuals with privileged access rights must constantly update and enhance their technical knowledge and other work-related skills, and share their knowledge and experiences with others.

3. Evidence of Trust

IS administrators with privileged access rights who are found not to comply with the IS Energy Benelux & Germany Policies, will lose their privileged access rights.