Final

Gedragscode voor IS-beheerders

Version	Version date	Author	Description of modifications	Owner
1.0	01/01/06	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. Inleiding

Bevoorrechte toegangsrechten stellen een persoon in staat om acties te ondernemen die een invloed kunnen hebben op de computersystemen, de netwerkcommunicatie of de accounts, bestanden, gegevens of procedures van andere gebruikers. Bevoorrechte toegangsrechten worden doorgaans toegekend aan systeem- of applicatiebeheerders, netwerkbeheerders, veiligheidspersoneel dat bij incidentenafhandeling betrokken is, of andere werknemers wier taken specifieke voorrechten m.b.t. een computersysteem of netwerk vereisen.

Personen met bevoorrechte toegangsrechten moeten de rechten van de gebruikers respecteren, de integriteit van de systemen en verwante fysieke bronnen bewaren en de van kracht zijnde beleidsnormen, wetten, regels en procedures naleven, waarbij ze ernaar streven die acties te ondernemen die vereist zijn om kwalitatieve, tijdige, betrouwbare en veilige computerdiensten te leveren.

Personen met bevoorrechte toegangsrechten zijn bijgevolg *verplicht om op de hoogte te blijven van* de procedures, bedrijfspraktijken en operationele richtlijnen die met de activiteiten van hun lokale departement verband houden. Alle beleidsnormen inzake veiligheid zullen worden bekendgemaakt in Blue Box (onder de sectie IS > Policies & Standards).

Informatie laten uitlekken of knoeien met informatie en computervoorzieningen kan niet alleen de individuele gebruikers of bedrijfsactiviteit nadelig beïnvloeden, maar in het geval van Business Area Energy Benelux & Germany kan dit ook een bedreiging vormen voor kritieke energie-infrastructuur.

Personen met bevoorrechte toegangsrechten moeten bijgevolg *betrouwbaar zijn, strenge ethische normen hanteren en een hoge mate van professionalisme aan de dag leggen* bij het uitvoeren van al hun taken.

2. Algemene bepalingen

1. Bevoorrechte toegangsrechten worden alleen aan gemachtigde personen toegekend en uitsluitend nadat een aanvraag werd ingediend en goedgekeurd.
2. Bevoorrechte toegangsrechten mogen alleen worden gebruikt om taken uit te voeren die door de hiërarchische manager of IS Energy Benelux & Germany-verantwoordelijke zijn opgelegd.
3. Indien acties met andere methodes dan met bevoorrechte toegangsrechten kunnen worden uitgevoerd, dan moeten die andere methodes worden gebruikt, tenzij de tijdsdruk of het gebruik van andere vereiste middelen duidelijk het gebruik van bevoorrechte toegangsrechten rechtvaardigen. In geval van twijfel moet het advies van de lokale Information Security Manager worden ingewonnen vooraleer actie wordt ondernomen.
4. Bevoorrechte toegangsrechten mogen uitsluitend worden gebruikt om aan een andere persoon middelen, toegang of voorrechten toe te kennen, te wijzigen of te weigeren indien het gaat om toegestane accountbeheeractiviteiten of in uitzonderlijke omstandigheden. Bij het uitvoeren van dergelijke acties moeten alle organisatorische richtlijnen en procedures strikt worden nageleefd.
5. In ieder geval moet elke toegang tot de elektronische informatie van andere personen (informatie over de e-mailaccount, details in verband met de berichten, internetlogs, enz.) beperkt blijven tot de minimale actie die noodzakelijk is om een situatie op te lossen, waarbij er zo weinig mogelijk inhoud mag worden doorgenomen.
6. Teneinde de vertrouwelijkheid te beschermen van de informatie die personen met bevoorrechte toegangsrechten bij het uitoefenen van hun taken te zien krijgen, dienen zij de nodige maatregelen te nemen, zowel op technisch vlak (bv. fysieke en technische vergrendelingen en veiligheidsmaatregelen) als op organisatorisch vlak (bv. procedures m.b.t. archivering en rapportering).

   Indien personen met bevoorrechte toegangsrechten bij het uitvoeren van hun taken per ongeluk

informatie zien die zou kunnen wijzen op een ongepast gebruik van informatietechnologie (bijvoorbeeld ongeoorloofde toegang, pogingen tot hacking), dienen zij onmiddellijk met hun lokale Information Security Manager te overleggen. Indien de situatie een onmiddellijke bedreiging vormt voor de informatiebeveiliging van Busines Area Energy Benelux & Germany, zou een onmiddellijke tussenkomst vereist kunnen zijn, zonder dat eerst met de lokale Information Security Manager kan worden overlegd. In dat geval moet de persoon met bevoorrechte toegangsrechten de lokale Information Security Manager zo snel mogelijk op de hoogte brengen van de bedreiging en van de acties die werden ondernomen.

7. Personen met bevoorrechte toegangsrechten moeten hun technische kennis en andere professionele vaardig¬heden voortdurend updaten en verrijken en zij moeten hun kennis en ervaring met anderen delen.

3. Bewijs van betrouwbaarheid

IS beheerders met bevoorrechte toegangsrechten van wie blijkt dat zij niet handelen overeenkomstig de gedragscodes van IS Benelux & Germany, verliezen alle rechten op bevoorrechte toegangrechten.