|  |
| --- |
| **Good practices procedure bescherming gegevens, activa en ICT** |
| Versie: april 2016Update: april 2017, oktober 2018 |
|  | OK | NOK |
| Het is raadzaam om maatregelen te treffen om de toegang tot kantoren en het kasgeld voor onbevoegden te verhinderen.Het is raadzaam om regelmatig een back-up te maken van de belangrijkste digitale informatie, die back-up kan best op een andere plaats dan de kantoren worden bewaard.Hierna volgen een aantal items die indien specifiek van toepassing als leidraad kunnen dienen/waarmee rekening kan gehouden worden om deze procedure op te stellen, uitbreidingen/expliciteringen op bepaalde punten of opname van particuliere gevallen zijn natuurlijk eveneens mogelijk en sterk aan te bevelen. Indien specifieke items opgenomen werden in het arbeidsreglement, gelieve dit hier te vermelden. |  |  |
| 1. **Beveiliging van kantoren (centraal secretariaat en regionaal steunpunt)**

Om de veiligheid van de werknemers en bezoekers beter te waarborgen, alsook om het risico op schade aan of diefstal van goederen van de HB te verminderen kunnen onder meer hiernavolgende items worden vermeld :* ligging (adres) van kantoren.
* vermelding van de openingsuren.
* wie heeft waar toegang tot welke ruimtes.
* is de toegang tot de gebouwen beveiligd met een alarminstallatie?

Wordt de toegang tot de kantoren en de arbeidsplaatsen via sleutels verzekerd of elektronisch gecontroleerd en/of worden er camera’s geïnstalleerd op de arbeidsplaatsen? Een elektronische toegangscontrole, alsook een camerabewaking wordt voorzien :* ter bescherming en veiligheid van de werknemers en bezoekers van de kantoren.
* ter bescherming van de eigendommen en goederen van de HB.

De ingevolge de elektronische toegangscontrole, alsook de camerabewaking bekomen gegevens kunnen enkel gebruikt worden in het kader van de beoogde doelstellingen, zijnde de bescherming en veiligheid van de werknemers en bezoekers van de arbeidsplaatsen en de bescherming van de eigendommen van de HB. Een beschrijving van de werking van de magneetkaarten en de hieraan gekoppelde software, alsook op welke wijze men omgaat met de verkregen data en beelden kan nader worden geëxpliciteerd.  |  |  |
|  |  |
| 1. **Beveiliging van het kasgeld/cheques**

Dit item kan overlappen/deels opgenomen zijn in een andere procedure (bv. kas- en liquiditeitenbeheer), gelieve dit hier te vermelden.  |  |  |
|  |  |
|  | OK | NOK |
| * De beveiliging van de kas houdt in dat de kas niet onbeheerd wordt achtergelaten en dat de bankbiljetten bijvoorbeeld in een brandkast worden gedeponeerd.
* Beschrijving van gebruik en beheer brandkast, koffers, kluizen (sleutels/codes, verantwoordelijken) en controle op gebruik en beheer ervan.
 |  |  |
| 1. **Beveiliging van digitale informatie**
* Elke pc-gebruiker dient zich te identificeren aan de hand van zijn gebruikersnaam en zijn wachtwoord.
* Tips en regels aan elke pc-gebruiker inzake de beveiliging van het wachtwoord, het regelmatig veranderen van wachtwoord, toegang tot internet …
* Reglement omtrent het gebruik van de digitale communicatiemiddelen.
 |  |  |
|  |  |
| 1. **Veiligheidsbeleid en toegang tot de KSZ**

De KSZ legt minimale normen op voor de gegevensbeveiliging aan alle organisaties die gebruik maken van informatie via de KSZ. De oprichting van een gegevensveiligheidsdienst die ervoor moet zorgen dat de gegevensveiligheid kan gewaarborgd en beheerd worden is één van de normen van de KSZ.* Toegang tot de KSZ : niet van toepassing voor de HB’s
 |  |  |
|  |  |
| 1. **Back-up van informatiesystemen**
* Beschrijving van de frequentie en de wijze waarop backups worden genomen, bewaard en gecontroleerd op de kwaliteit.
* Een gedetailleerde lijst bijgehouden (door de systeemverantwoordelijke) wanneer een back-up is genomen, identificatie van de media, aanduiden wat het resultaat was (OK, gedeeltelijk OK - met een uitleg, mislukt). Hierin worden ook elke restore operatie en alle testen genoteerd, met inbegrip van het resultaat.
* De ICT systeemverantwoordelijke zal dagelijks de logfiles nazien en maatregelen nemen indien blijkt dat de kwaliteit van het back-up proces te wensen over laat.
* Reglement omtrent de toegang tot de servers en de beveiliging ervan.
 |  |  |
|  |  |
|  | OK | NOK |
| 1. **Schematische voorstelling verantwoordelijkheden m.b.t. de procedure**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Fase** | Pers | Co | Vz | **RvB** |
| 1 | Ontvangst sleutel en toegangscode gebouw (kantoor, …) |  |  |  |  |
| 2 | Afsluiten gebouw (kantoor, …) en activeren alarmsysteem |  |  |  |  |
| 3 | Teruggave sleutel en desactiveren toegangscode |  |  |  |  |
| 4 | Opmaak gebruikersnaam en paswoord pc |  |  |  |   |
| 5 | Login voor specifieke toepassingen |  |  |  |  |
| 6 | Aanpassen procedure … |  |  |  |  |
|  | … |  |  |  |  |

 |  |  |
|  |  |
| **Beoordeling:**De procedure bescherming van gegevens, activa en ICT is niet goed/voor verbetering vatbaar/goed. |  |  |