Strategisch meerjarenplan informatieveiligheid

2014 - 2017

Versie	Datum	Auteur(s)	Wijziging	Status
0.1	03/02/2014	Verleijen Jacques		Voorstel
0.2	26/02/2014		Aanpassingen na DiRa	goedgekeurd
1.0	04/04/2014		Raad van het GO!	Goedgekeurd

20-3-2014
Stafdiensten
Huis van het GO!
Willebroekkaai 36
1000 Brussel

Inhoudsopgave

Mission statement

Het GO! wil de nieuwe informatie- en communicatietechnologie toegankelijk en beschikbaar maken voor iedereen, met respect voor privacy, de specifieke wet- en regelgeving en conform haar pedagogisch project. Daarom moet de beschikbare informatie op een veilige manier behandeld worden.

Informatieveiligheid is meer dan het implementeren van technische oplossingen; zij steunt vooral op het bewust maken van alle personeelsleden binnen het GO! zodat zij dit beleid begrijpen, steunen en toepassen.

In die zin streeft het GO! naar een geïntegreerde systeemaanpak, met als resultaat dat de risico's voor de confidentialiteit, de integriteit, authenticiteit en beschikbaarheid van de informatiebronnen en -systemen tot een minimum beperkt blijven.

Het GO! zal zijn veiligheidsbeleid ontwikkelen in overeenstemming met de ISO27000 normen en de richtlijnen van de Vlaamse Gemeenschap.

Voor de uitwerking van dit beleid verwijzen we naar de beleidsverklaring voor informatieveiligheid van het GO! die wordt opgevolgd door de stuurgroep "Informatieveiligheid" en gecoördineerd door de informatieveiligheidsconsulent.

0. Woord vooraf

Met het in gebruik nemen van ons nieuw “Huis van het GO!” zijn we ook een nieuw tijdperk ingetreden wat betreft informatieveiligheid. Dit betekent op dit vlak ook een “big bang”. De zaak is nu om deze verwezenlijkingen te behouden. Dit is opgenomen in dit meerjarenplan.

Tevens moeten wij onze aandacht verschuiven naar de meso- en microniveau. Ook daar wordt het beveiligen van persoonsgegevens een belangrijke topic.

Het is met gemengde gevoelens dat ik een meerjarenplan moet schrijven waarvan ik de volledige verwezenlijking niet zal meemaken. Maar ik wil mijn opvolger ook niet confronteren met een grote duik in het onbekende.

Ik overweeg dus ook om mijn pensioenaanvraag met één jaar uit te stellen om de aanzet van dit meerjarenplan in goede banen te leiden.

Jacques Verleijen – Informatieveiligheidsconsulent

Brussel 10 februari 2014

1. Actualisering beleidsverklaring

De huidige beleidsverklaring dateert van september 2011. Ze werd goedgekeurd door de DiRa en door de Raad van het GO respectievelijk op 16 maart en 23 september 2011.

Ondertussen is de situatie waarin we verkeren grondig veranderd:

- Het in gebruik nemen van het “Huis van het GO!” was tevens de aanleiding om het nieuwe werken te introduceren. Naast de vernieuwing van de ICT infrastructuur worden ook nieuwe werkprocessen geïntroduceerd.
- Het gebruik van nieuwe communicatie technologieën tussen het Departement Onderwijs en de instellingen (zoals Da Vinci en Discimus) maken dat de Vlaamse Toezichtscommissie vereist dat ook onderwijsinstellingen aandacht schenken aan de informatieveiligheid.
- De huidige beleidsverklaring blijkt niet meer in overeenstemming te zijn met de realiteit op het veld.

Om die redenen moet deze beleidsverklaring worden aangepast.

Timing:
Voorstel aan DiRa: woensdag 2 april 2014
Voorstel aan Raad van het GO! juni 2014

Budget: nihil

2. Centrale diensten

2.1. Situering

Met het in gebruik nemen van ons nieuw Huis van het GO! hebben we een reuzenstap gezet in verband met informatieveiligheid en kwaliteit die we kunnen bieden. Wij kunnen nu model staan voor heel wat Vlaamse en federale overheidsdiensten.
De zaak is nu het consolideren van de onze huidige voorsprong.
Dit deel van het meerjarenplan is opgemaakt in nauw overleg met de ICT manager, zowel wat de strategische doelstellingen betreft als de budgettaire weerslag ervan.

2.2. Auditeren van de nieuwe ICT infrastructuur

Vorig jaar werden onze externe websites getest door een Ethical hacker op hun zwakheden. Er werden ook penetratietesten uitgevoerd op de op de testomgeving van de VDI. Bij de nieuwe ICT infrastructuur werd rekening gehouden met de resultaten van deze tests.
Het overzetten van de oude naar de nieuwe ICT infrastructuur moet afgewerkt zijn voor 30 juni 2014.
Als deze nieuwe infrastructuur volledig operationeel zal zijn is het aangewezen om deze terug te testen op externe en interne bedreigingen.

Timing:
Offerte: april – mei 2014
Uitvoering: Juli – augustus 2014
Rapportage: september 2014
Bijsturing: september – december 2014

Budget: € 9000 (voorzien)

2.3. ISO 27001 certificering van de ICT dienst

Zoals reeds gezegd in het eerste punt is onze infrastructuur een voorbeeld voor anderen. Op het vlak van procesbeheer zijn we ook op de goede weg. Veel processen worden verbeterd, maar zijn nog niet geborgd.
Een ISO certificering verplicht een organisatie om zijn processen te beschrijven, te bewaken en te verbeteren.
Op het vlak van informatiebeveiliging vraagt de overheid en de controlerende instanties (CBPL en VTC) steeds meer waarborgen. Een ISO 27001 certificaat waarborgt onze “klanten” en de overheid dat we informatieveiligheid ernstig nemen.
Dit moet op lange termijn gepland worden door de scoop goed af te bakenen en stelselmatig uit te breiden. Daarom beperken we ons in een eerste fase tot de ICT dienst, zowel wat de dienstverlening betreft en de productie.
ICT dienstverlening:

- Helpdesk
- Netwerkbeheer
- Onderhoud van systemen
- Toegangsbeheer

ICT productie:

- Beheer en onderhoud van websites
- Ontwikkeling van eigen software, al dan niet in onder aanneming

Deadline: 30 juni 2015

Timing:
- Scopebepaling: maart 2014
- Analyse: april – juni 2014
- Voorbereiden documenten: september – november 2014
- Consultancy: november 2014 – maart 2015
- Preaudit: februari 2015
- Audit: maart 2015

Dit geeft ons drie nog drie maand om eventuele afwijkingen te corrigeren.

Budget:
- Audit : € 3000
- Consultancy: € 5000 (waarvan € 2000 in 2014)
- Opleiding: € 2900

2.4. Continuïteit management

Er was een noodplan in verband met ICT problemen in ons oud gebouw. Er bestaat ook een BCP (Bussines Continuity plan) voor de migratie van de oude ICT infrastructuur naar onze nieuwe servers. In 2014 moet er een BCP gemaakt worden voor de nieuwe IT infrastructuur door één van de projectleiders.
Los daarvan moet er ook een Business Continuity Management plan worden opgesteld voor onze organisatie. Daarin moeten de kritische business processen gedefinieerd worden. Van deze processen moet vastgelegd worden wat de maximale uitvaltijd mag zijn en hoe de dienstverlening kan gewaarborgd worden. Deze oefening dient per afdeling te gebeuren.

Timing:
- BCP ICT: December 2014 (nodig voor de ISO certificatie)
- Kick off BCP andere afdelingen: September 2014
- Einde: December 2016

Budget:
Nihil, wel tijdsinvestering (projectmanager ICT en tijdsinvestering per afdeling)

2.5. Uitbreiding van de ISO 27001 certificering

Indien de DiRa opteert om testreven naar een ISO certificering dan kan de scope uitgebreid worden naar andere diensten van het GO! centraal.
Dit gebeurt het best stapsgewijs, zeker wat de voorbereiding betreft. Dit vergt analyse van de processen, het ontwerpen en uitschrijven van de nodige documenten en procedures. De ICT dienst kan als voorbeeld gelden.
De informatieveiligheidsconsulent kan dan het best een opleiding volgen als “ISO 27001 implementer” om zo de kosten van een externe consultant uit te sparen.

Timing:
- Opleiding IVC: begin 2015
- Kick-off: te bepalen per afdeling, maar niet voor augustus 2015
- Certificering: 2017

Budget:

- Opleiding: € 2900
- Jaarlijkse audit: € 4000

3. Mobile device management

3.1. Situering

Het open karakter van het Huis van het GO! maakt dat veel mensen hier komen met hun eigen materiaal. Meer en meer personeelsleden maken ook gebruik van hune eigen tablet of smartphone. Dit kan een risico betekenen voor het interne netwerk.
Scholen worden ook met deze problematiek geconfronteerd en ook daar is vraag naar een betere beveiliging.

3.2. Aankoop en installatie

Er bestaat op de markt software die het beheer van eigen toestellen en die van bezoekers kunnen beheren. Dit noemt men Mobile Device Management.
We gaan dus op zoek naar een raamcontract waar de scholen(groepen) kunnen op intekenen. Daarbij moet ook de nodige aandacht besteed worden aan de opleiding voor het gebruik en het beheer van de toepassing.

Timing:
Februari-maart 2014: onderzoeken of dit kadert in de raamovereenkomst met Onderwijs.
Indien wel:

- Implementatie in het huis van het GO!: april – juni 2014
- Voorbereiden communicatie naar scholengroepen: april-mei 2014
- Implementatie in SGR: volgend schooljaar
- Verdere opvolging: 2015-2017

Indien niet:

- Opstellen lastenboek: maart-april 2014
- Publiceren en intekenen: vereenvoudigde procedure met bekendmaking (eind april)
- Beslissing: eind juni- begin juli 2014
- Implementatie volgend schooljaar
- Uitrol naar de SGR 2015 -2017

Budget: is voorzien bij ICT-dienst wat betreft de centrale diensten. Voor de scholengroepen moet dit nog besproken worden.

4. Uitrol naar de scholen(groepen)

4.1. Situering

Met de invoering van de nieuwe communicatiestromen tussen het Departement Onderwijs en onze instellingen (scholen, CVO's en CLB's) heeft de Vlaamse Toezichtscommissie en de Privacy Commissie ook bepaalde veiligheidseisen geëist aan deze instellingen.
De onlangs verruimde bevoegdheden van het VTC (6/12/2013) zijn van die orde dat er meer aandacht moet gegeven worden aan de beveiliging van persoonsgegevens.
Onze scholen en centra moeten dus ook werk maken van het beschermen van hun gegevens. De directies moeten bewust gemaakt worden van de risico's die ze lopen en de mogelijke gevolgen voor hun instelling.

4.2. Informatie aan de scholengroepen

In een eerste fase moeten de algemene directeurs, de directeurs en de kaderleden van de scholengroepen geïnformeerd worden over de gewijzigde situatie en de mogelijkheden die we gaan bieden aan de scholen(groepen);
Dit kan via de colleges van directeurs of de lerende netwerken.

Timing:

- Voorstelling aan de CoRa: april- mei 2014
- Deelname aan de lerende netwerken: mei- juni
- Op vraag: toelichting aan colleges van directeurs (2014 -2017)

Budget: verplaatsingskosten

4.3. Opleiding directies

Gezien het groeiend belang van de informatiebeveiliging op school en de grotere verantwoordelijkheid van de directies; moet er een verplichte opleidingsmodule komen die deze aspecten belicht.

Timing:

- Opname in verplichte module: onderhandelen met NAS/PBD: maart – juni 2014
- Voorbereiding vorming: september-oktober 2014
- Geven van opleiding: volgend schooljaar
- Dezelfde module kan ook aangeboden worden in de nascholing van het NAS (vaste datum en op vraag)

Budget: verplaatsingskosten

4.4. Audits ter plaatse

Op vraag van het Departement Onderwijs werden de CVO's vorig schooljaar geconfronteerd met de vraag om een risicoanalyse uit te voeren om de beginsituatie vast te leggen. Dit staat ook aan te komen op het niveau van de scholen, CLB's en scholengroepen.
Daarvoor werd door ons een audittool ontwikkeld, om de instellingen te helpen hun situatie in kaart te brengen.
Deze audits gebeuren best te plaatse en zijn conform de ISO 27002 norm. Het is niet de bedoeling om scholen(groepen) te certificeren, maar om deze internationaal erkende norm zo goed mogelijk te benaderen. Het departement onderwijs hanteert ook deze norm.

Timing

- Voorstel aan Cora en SGR: zie 4.2
- Audits : september 2014 – 2017

Budget: verplaatsingskosten