Bijlage 2 Implementatieplan FitNu

Opdrachtgever: R. de Vries

Datum: 21-05-2019

Auteur: J. de Ridder, R. Hattem en Ritwan Gaasim

Versie: 1.0

INHOUD

[1 Inleiding 3](#_Toc535608921)

[2 Implementatiegegevens 3](#_Toc535608922)

[2.1 Opdrachtgever 3](#_Toc535608923)

[2.2 Projectteam en betrokkenen 3](#_Toc535608924)

[2.3 Knelpunten in huidige situatie 3](#_Toc535608925)

[2.4 Gewenste situatie 3](#_Toc535608926)

[3 Gevolgen van de implementatie 10](#_Toc535608927)

[3.1 Organisatorische gevolgen 10](#_Toc535608928)

[3.2 Technische gevolgen 11](#_Toc535608929)

[4 Aanpak en planning 11](#_Toc535608930)

[5 Uit te voeren activiteiten 11](#_Toc535608931)

[6 Testrapportage 12](#_Toc535608932)

[7 Risico’s en bedreigingen 12](#_Toc535608933)

[8 Toekomst 12](#_Toc535608934)

[9 Acceptatie en overdracht 12](#_Toc535608935)

[10 Communicatie met opdrachtgever 12](#_Toc535608936)

# Inleiding

Dit implementatieplan beschrijft de implementatie van de nieuwe ICT-infrastructuur voor Fitness Organisatie FitNu. Het implementatieplan is tot stand gekomen na overleg met alle betrokkenen.

# Implementatiegegevens

## Opdrachtgever

Fitnessorganisatie FitNu is gevestigd te Amsterdam.

## Projectteam en betrokkenen

Betrokkenen zijn:

* R. de Vries, directeur van FitNu
* J. de Ridder, systeembeheerder van FitNu, projectleider Implementatie FitNu
* R. Hattem, systeembeheerder van FitNu
* WeConnectYou, externe ICT-specialist
* R.Gaasim, Lid van het projectteam

## Knelpunten in huidige situatie

In de huidige situatie is de ICT-infrastructuur volledig geleased van een derde partij. Dit is bedoeld als overgangssituatie. Deze tijdelijke situatie moet nu omgezet worden naar een definitieve situatie waarin de apparatuur in eigendom komt van FitNu. De technische verbindingen van de netwerkinfrastructuur worden gedelegeerd naar het ICT-bedrijf WeConnectYou te Amsterdam. Het projectteam richt zich vooral op de implementatie van de domeinomgeving en de configuratie van de Active Directory.

## Gewenste situatie

De gewenste situatie is als volgt:

* De netwerkconfiguratie van alleen de werkstations dient vanuit een centraal punt te worden gedistribueerd.
* Alle medewerkers krijgen een home directory op de centrale fileserver in Amsterdam. Er mogen geen documenten meer op de lokale werkstations worden opgeslagen. De home directory moet worden voorzien van de drive letter H. De verbinding naar de fileserver moet veilig zijn.
* Documenten worden per afdeling (Management, Financiën, Administratie en Receptie, Sportmedisch, ICT-beheer, Techniek, Fitness Instructeurs, Personal Trainers) opgeslagen op de centrale fileserver.
* Alle medewerkers moeten toegang krijgen en leesrechten op alle afdelingen.
* De medewerkers krijgen lees- en schrijfrechten op hun eigen afdeling.
* Het management krijgt lees- en schrijfrechten op alle afdelingen behalve de sportmedische.
* De documenten van alléén het management dienen bij voorkeur encrypted te worden opgeslagen en mogen nooit offline beschikbaar worden gesteld.
* Het management krijgt vanaf elke externe locatie toegang tot de fileserver via een beveiligde internetverbinding.
* Centraal opgeslagen bestanden zoals telefoon- en adreslijsten van medewerkers en cliënten zijn offline beschikbaar op alle werkstations en zijn toegankelijk voor alle medewerkers inclusief de receptie.
* Alle medewerkers dienen in eenheden (per afdeling, zie punt 3) te worden georganiseerd.
* Iedere eenheid krijgt een eigen beheerder voor eenvoudige taken, zoals het veranderen van het password of het toevoegen of veranderen van een gebruikersaccount. Het hoofd van de afdeling (de eerstgenoemde persoon) wordt de gedelegeerde beheerder.
* Geef de gedelegeerde beheerder een snap-in tool (MMC: met een uitgeklede versie van Active Directory Users and Computers) Deze tool moet op het werkstation van de gedelegeerde beheerder kunnen worden uitgevoerd.
* De afdelingen Fitness Instructeurs en Personal Trainers mogen op hun werkstation niets veranderen aan de instellingen van hun systeem.
* Elk werkstation krijgt een vaste desktopafbeelding (zie hiernaast) die niet door de gebruiker mag worden aangepast. Deze desktopafbeelding wordt gedistribueerd.
* Elke afdeling krijgt per vestiging een eigen printer en deze dient automatisch als standaardprinter te worden toegevoegd aan werkstations.
* Bij een printopdracht dient het hoofd van elke afdeling voorrang te krijgen op de printopdrachten van andere medewerkers van die afdeling.
* De instructeurs mogen geen software installeren op hun werkstation.
* De rekenmachine calcplus.msi dient als extra programma centraal beschikbaar te worden gesteld en geïnstalleerd op alle werkstations van de medewerkers van Techniek.
* Het wachtwoord moet voldoen aan alle eisen.
* Het wachtwoord mag niet de laatste 12 keer al gebruikt zijn.
* Alle medewerkers vernieuwen elke 30 dagen hun wachtwoord.
* De minimale wachtwoordlengte moet 10 tekens zijn.
* Wachtwoorden moeten een sterke beveiliging hebben en voldoen aan de eisen van de complexity requirements.
* Er wordt bijgehouden wie vanaf een bepaald werkstation geprobeerd heeft om oneigenlijk toegang te verkrijgen tot vertrouwelijke sportmedische bestanden.
* De fileserver wordt beschermd tegen calamiteiten. Een gebruiker kan zelf de voorgaande versie van een bestand terughalen.
* De domeinomgeving wordt beschermd tegen het uitvallen van een fysieke component. Het is wenselijk een Domain Controller te plaatsen in zowel Amsterdam als in Utrecht. De communicatie tussen beide computers is veilig.

#### Topologie Netwerk

De nieuwe configuratie van de netwerkinfrastructuur van FitNu wordt verdeeld over de locaties Amsterdam en Utrecht. In de toekomst zal Arnhem worden toegevoegd. De implementatie van de technische verbindingen van de netwerkinfrastructuur zullen worden gedelegeerd aan het externe ICT-bedrijf WeConnectYou uit Amsterdam. De contactpersoon is mevrouw A. Verhulst.

De gedetailleerde functionele opdracht aan WeConnectYou moet nog worden opgesteld. Dit betreft het aanpassen en het onderhoud van de lokale netwerkinfrastructuur (LAN topologie) en het gerouteerd verbinden van de locaties Amsterdam en Utrecht (WAN topologie).

#### Domain Services

Op basis van de implementatie-eisen (zie Bijlage 1) hebben wij de volgende technische gegevens betreffende de domein-configuratie kunnen vaststellen.

#### Domain- en naamgevingsstructuur

Domeinnaam : FITNU.LOCAL

#### Computernamen

* Domain Controllers: DCxx
* Servers: SRVxx
* Werkstations: WSxx
* Laptops: LAPxx
* Printers: PRNxx
* Routers: RTxx
* Switches: SWxx
* Cardio-apparatuur CDXX

Voor de locatie Utrecht wordt –U toegevoegd aan de namen bijvoorbeeld WS01-U.

Voor de locatie Amsterdam wordt –A toegevoegd aan de namen bijvoorbeeld WS01-A.

#### Vestiging Amsterdam

Server

**DC01-A**

*DC01-A.FITNU.LOCAL* heeft de serverrollen DNS, AD DS met de volgende instellingen.

**AD DS**

Het unattended script ziet er als volgt uit.

* + [DCInstall]
  + New forest promotion
  + ReplicaOrNewDomain=Domain
  + NewDomain=Forest
  + NewDomainDNSName= *FITNU.LOCAL*
  + ForestLevel=2
  + DomainNetbiosName= *FITNU*
  + DomainLevel=2
  + InstallDNS=Yes
  + ConfirmGc=Yes
  + CreateDNSDelegation=No
  + DatabasePath="C:\Windows\NTDS"
  + LogPath="C:\Windows\NTDS"
  + SYSVOLPath="C:\Windows\SYSVOL"
  + Set SafeModeAdminPassword to the correct value prior to using the unattend file
  + SafeModeAdminPassword=Welkom01
  + RebootOnCompletion=Yes

**DNS**

* Secure only
* Active Directory Integrated

**IP-configuratie**

* IP: 10.0.20.10
* Subnetmask: 255.255.255.0
* Gateway: 10.0.20.1

#### Vestiging Utrecht

Server

**DC02-U**

*DC02-U.FITNU.LOCAL* heeft de serverrollen AD DS, DNS met de volgende instellingen.

**AD DS**

* Domeincontroller in het domein FITNU.LOCAL

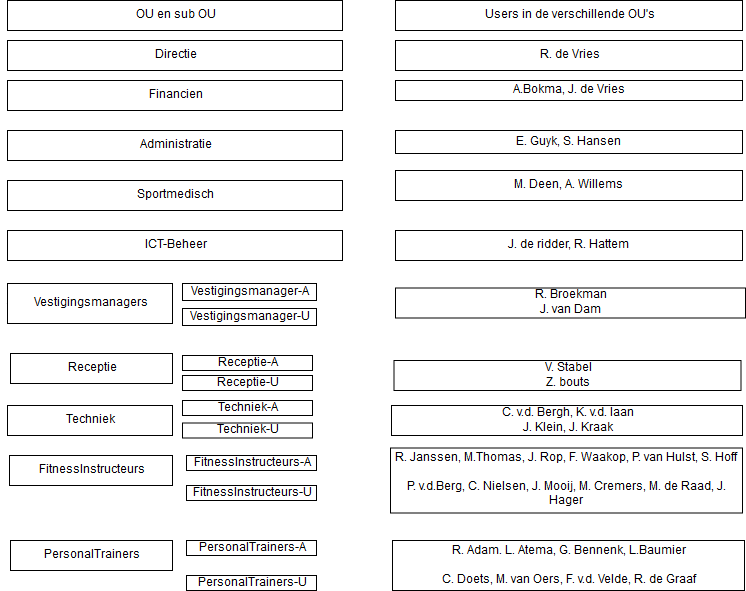
**DNS**

* Secure only
* Active Directory Integrated

**IP-configuratie**

* IP: 10.0.20.11
* Subnetmask: 255.255.255.0
* Gateway: 10.0.20.1

**OU structuur**



Ik heb voor deze structuur gekozen omdat het op deze manier overzichtelijk is wie bij welke afdeling hoort. Hierdoor is het ook makkelijker om mensen rechten te geven en policies toe te passen.

#### Naamgeving AD-objecten

Er wordt gekozen voor het volgende format voor de gebruikersnamen.

**[voorletter][.][volledige achternaam] met eventueel een volgnummer[xx]** indien er sprake is van een dubbele achternaam.

Bij het toekennen van permissies aan (file en printer) resources zal van toepassing zijn het principe:

**A -> GG -> DL <- P**

Users plaatsen in een Global Group (GG) en deze plaatsen in een groep Domain Local (DL). Vervolgens Permissies toekennen aan de DL.

Voor de naamgeving van de groepen spreken we af:

* Global Groups krijgen een naam die betrekking heeft op het type accounts en zal beginnen met GG (bijvoorbeeld GGictbeheer).
* Domain Local groups krijgen een naam die betrekking heeft op het type resource en zal beginnen met DL (bijvoorbeeld DLPrinterSportMedisch).

#### GPO instellingen

#### Aan te brengen policies

|  |  |
| --- | --- |
| Functionele eis 1 | Configuratiescherm en PC settings |
| Voor wie | Afdeling Fitness Instructeurs, Personal Trainers |
| Policy name | Prohibit access to Control Panel and PC settings |
| Setting | * Enabled * Geen toegang tot configuratiescherm |

|  |  |
| --- | --- |
| Functionele eis 2 | Home Directory |
| Voor wie | Alle werknemers |
| Policy name | Set user home folder |
| Setting | -Enabled  -Location On the network  -Path [\\Servernaam\\users$](file:///\\Servernaam\\users$)  -drive letter H: |

|  |  |
| --- | --- |
| Functionele eis 3 | Forceer desktop wallpaper op alle werkstations |
| Voor wie | Alle werknemers |
| Policy name | Desktop Wallpaper |
| Setting | -Enabled  -Pad aangeven waar de afbeelding zich bevindt |

|  |  |
| --- | --- |
| Functionele eis 4 | Calcplus.msi op alle werkstations |
| Voor wie | Alle werknemers |
| Policy name | Software installation |
| Setting | -calcplus.msi uitrollen over het netwerk dat bij inloggen het programma op het werkstation staat. |

|  |  |
| --- | --- |
| Functionele eis 5 | Software mag niet geinstalleerd worden |
| Voor wie | Instructeurs |
| Policy name | Turn off Windows Installer |
| Setting | -Gebruiker kan geen software op het werkstation zetten |

|  |  |
| --- | --- |
| Functionele eis 6 | Wachtwoord policy |
| Voor wie | Alle werknemers |
| Policy name | Password policy |
| Setting | -Maxim password age  -Minimum password age  -Minimum Password length  -Password must meet complexity requirements |

|  |  |
| --- | --- |
| Functionele eis 7 | Bijhouden wie toegang probeert te krijgen tot bestanden |
| Voor wie | Alle werknemers |
| Policy name | Audit object access |
| Setting | -Houd bij in de event viewer wie toegang krijgt of probeert te krijgen tot bestanden. |

#### File en Printserver

*[Richt de fileserver en printserver in volgens Bijlage 1 Implementatie-eisen.]*

De server SRV01-A wordt ingericht voor de opslag van gezamenlijke documenten, persoonlijke documenten van de werkstations (Folder Redirection policy).

Op SRV01-A wordt de volgende mappenstructuur aangebracht voor de gedeelde documenten.

*[Richt de fileserver in op basis van informatie uit Bijlage 1 Implementatie-eisen.]*

Voor de persoonlijke bestanden zal de Folder Redirection policy worden aangemaakt. Voor elke username wordt een map genaamd ***\\SRV01-A\home\%username%*** ingericht. Ook zal deze server worden gebruikt voor de centrale opslag van de persoonlijke gebruikersprofielen in de map [**\\SRV01-A\profile\%username%**](file:///\\SRV01-A\profile\%25username%25). Iedere afdeling krijgt zijn eigen share onder **\\SRV-01\afdelingen\**. Als voorbeeld: de afdeling “trainers” krijgt **\\SRV-01\afdelingen\trainers\** als share.

#### Rechtenstructuur folders

|  |  |  |
| --- | --- | --- |
| **Afdeling** | **Share name** | **Share - NTFS Permissie(s)** |
| Trainers | trainers | trainers – F instructeurs – RE financien – N techniek – N  sportmedisch – N  management - RE administratie - N ictbeheer - N |
| Financiën | Financiën | trainers – N instructeurs – N financien – F techniek – N  sportmedisch – N  management - RE administratie - RE ictbeheer – N |
| Techniek | Techniek | trainers – N instructeurs – N financien – N techniek – F  sportmedisch – N  management - RE administratie - N ictbeheer - RE |
| Sportmedisch | Sportmedisch | trainers – N instructeurs – N financien – N techniek – N  sportmedisch – F  management - N administratie - N ictbeheer - N |
| Management | Management | trainers – RE instructeurs – RE financien – RE techniek – RE  sportmedisch – N  management - F administratie - RE ictbeheer - R |
| Administratie | Administratie | trainers – N instructeurs – NE financien – RE techniek – N  sportmedisch – N  management - RE administratie - F ictbeheer – N |
| ICT-beheer | ICT-beheer | trainers – N instructeurs – N financien – N techniek – N  sportmedisch – N  management - RE administratie - N ictbeheer – N |
| Afdelingen | Afdelingen | trainers – R instructeurs – R financiën – R techniek – R  sportmedisch – R management – R&E administratie - R ictbeheer – R |
| Home | Home | Home directory is voor iedereen voor zichzelf toegankelijk niemand anders mag daarbij komen. |
| Profiles | Profiles | trainers – N instructeurs – N financiën –N techniek – N sportmedisch – N  management – N administratie - N ictbeheer – F |
| NTFS permissions: F = Full Control - M = Modify - RE = Read & Execute - R = Read - W = Write - N = Geen | | |

# Gevolgen van de implementatie

## Organisatorische gevolgen

Voor de organisatie moeten de beheerders van elke OU een cursus krijgen welke taken zij bij hun werkzaamheden krijgen als beheerder . Bijv. wachtwoorden veranderen. Ook moet het management uitleg krijgen hoe ze contact kunnen leggen met de server door middel van VPN.

Hieronder volgt een overzicht wie de beheerder is van de desbetreffende OU:

|  |  |  |  |
| --- | --- | --- | --- |
| **OU** | **Beheerder** | **SubOU** | **Beheerder** |
| Financien | A. Bokma | - | - |
| Sportmedisch | M. Deen | - | - |
| Vestigingsmanager | - | Vestigingsmanager-a Vestigingsmanager-u | R. Broekman J. van Dam |
| FitnessInstructeurs | - | FitnessInstructeurs-a FitnessInstructeurs-u | R. Janssen P. v.d. Berg |
| ICT-Beheer | J. de Ridder | - | - |
| Directie | R. de Vries | - | - |
| Receptie | - | Receptie-A Receptie-U | V.Stabel Z.Bouts |
| Techniek | - | Techniek-A Techniek-U | C. v.d. Bergh J. Klein |
| PersonalTrainers | - | PersonalTrainers | PersonalTrainers-A PersonalTrainers-U |
| Administratie | E. Guyk | - | - |

## Technische gevolgen

De VPN-verbinding word gedelegeerd naar WeConnectYou. Zij zullen alle netwerk gerelateerde zaken op zich nemen. Elke afdeling krijgt zijn eigen printer. Deze zal ingesteld zijn als standaard printer op het werkstation. De techniek lost problemen op op de werkvloer als er iets mis is met fitness aparatuur. De ICT-beheerders zijn verantwoordelijk voor alle ICT gerelateerde zaken.

1. Aanpak en planning

Dit project wordt volgens een standaard projectmethodiek aangepakt. De fasering is als volgt.

1. Initiatieffase; definitiefase; ontwerpfase
2. Voorbereidingsfase; uitvoeringsfase; nazorgfase

De eerste stap is afgerond, de implementatie begint met stap 2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Volgnr.** | **Activiteit** | **Consequenties** | **Uitvoerder** | **Geschatte implementatietijd** |
| 1 | Voorbereidingsfase | Implementatieplan schrijven | R. Gaasim | 3 uur |
| 2 | Uitvoeringsfase | Het implementatieplan uitvoeren. Dat gemaakt is van tevoren. | R. Gaasim & WeConnectYou | 3 uur |
| 3 | Nazorgfase | Tests gebaseerd op de wensen | R. Gaasim | 1 uur |
|  |  |  | Totaal | 7 uur |

1. Uit te voeren activiteiten

**Uitvoeringsfase:**

**WeConnectYou:**

WeConnectYou regelt alle netwerkgerelateerde zaken. Onder andere de VPN verbinding voor het management, de DHCP-server en de verbinding tussen de server in Amsterdam en Utrecht.

**Projectteam FitNu:**

**De installatie van de AD.**

* Let op juiste domeinnaam

**Toevoegen van OU’s**:  
De OU’s zijn beschreven in dit implementatieplan. De OU’s hoeven alleen aangemaakt te worden met de users en groepen erin. Elke OU krijgt zijn eigen beheerder.

* Juiste naamgeving van de OU’s
* De gebruikers in de juiste groepen zetten

**GPO’s instellen**:  
De GPO’s verschillen per afdeling niet alle GPO’s gelden voor iedereen let dus op dat:

* De GPO’s niet op de default policy zetten als het niet geld voor het hele domein.
* Zet de juiste GPO’s op de juiste OU.

**Offline bestanden beschikbaar stellen:**  
Centraal opgeslagen bestanden moeten offline beschikbaar zijn.  
**Shares aanmaken:**

Elke afdeling krijgt zijn eigen share voor bestandsopslag. De gebruikers moeten ook rechten toegewezen krijgen.  
  
**Printers instellen voor de users:**  
Elke afdeling krijgt zijn eigen printer. Let op dat de prioriteit per printer anders is.

**DHCP-Server:**

Een DHCP-server op te zetten voor onze werkstations. Hierdoor krijgen de werkstations een IP-adres toegewezen en hoeven wij dit niet handmatig in te stellen.

**2de Domain Controller**

2de Domain Controller plaatsen in Utrecht. De verbinding moet ook veilig zijn tussen de computers.

**VPN**  
VPN verbinding opzetten zodat de server altijd bereikbaar is voor de management medewerkers.

**Nazorgfase:**

Voor iedere wens moet een test opgesteld worden. Sommige wensen kunnen bij elkaar gezet worden en er 1 test van gemaakt worden.

# Testrapportage

De technische testen en acceptatietesten worden beschreven in de testrapportage FitNu, Bijlage 5 *Sjabloon Checklist en Testrapportage*.

# Risico’s en bedreigingen

Bij het installeren van het AD moet je ingelogd zijn als een administrator. De administrator moet ook een wachtwoord hebben anders gaat de installatie niet lukken. Bij de GPO’s moet er goed opgelet worden dat deze juist staan ingesteld.

# Toekomst

In het ontwerp is gebruikgemaakt van moderne technieken en rekening gehouden met bedrijfsveranderingen. Toch zijn er mogelijk ontwikkelingen in de nabije toekomst die deze infrastructuur kunnen beïnvloeden.

In Arnhem kan er in de toekomst een vestiging bij komen. Hiervoor kunnen dan nieuwe OU’s aangemaakt worden. Eventuele nieuwe printers zullen dan er ook bij worden geze. Nieuwe gebruikers kunnen ook op de server worden toegevoegd. Arnhem zal ook zijn eigen AD krijgen die kan aan het bestaande domein worden toegevoegd.

# Acceptatie en overdracht

De testen voor acceptatie vinden plaats op basis van Bijlage 1 *Implementatie-eisen FitNu*. Daarna worden afspraken gemaakt voor de overdracht en de evaluatie van de implementatie.

# Communicatie met projectleider

Bespreek met de projectleider de evaluatie van het implementatieplan en verwerk de op- en aanmerkingen mee in de evaluatie van het implementatieplan.