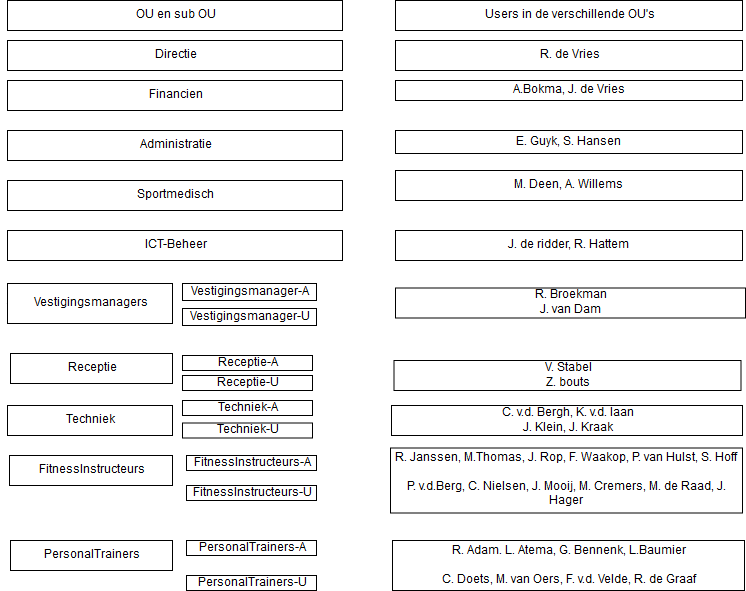
## Gewenste situatie

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.
* *[Beschrijf de te delegeren onderdelen op basis van informatie uit Bijlage 1 Implementatie-eisen, punten 1, 4 en 16.]*

*Ou:*



Gpo:

|  |  |
| --- | --- |
| 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. |

|  |  |  |
| --- | --- | --- |
| **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 | | |

## 3.1Organisatorische 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 | - | - |

## 3.2Technische 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.

4.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 | 1. uur |

5. 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.

# 7Risico’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.

1. 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.

Azure ad of onedrive erbij?