Service Agreement

Virtual Research Workspace (VRW)

Document 1.0
Author: A.R.J.Liemberg; R.Posthuma
Date 05012019
Service Agreement
Virtual Research Workspace

Table of Contents

Service description 2
For whom 2
Customer value 2
What do we offer? 2
Usage 2
Service owner 3
Security & privacy 3
Storage & backup 3
Account administration 3
Data transport 4
Desktop applications 4
System management 4
Support 5
Configuration & Performance 5
Finance 5
Connected services 6

Appendix 1 Servicelevels 6

Appendix 2 Information Security Baseline 8
Service Agreement

Virtual Research Workspace

Service description
The virtual research workspace consists of a virtualized desktop environment where researchers can conduct data analyses jointly and securely. In this workspace, partnerships are possible with researchers from within the organization itself or from other institutions worldwide. These services (applications & data) are available 24/7. The virtual environment can be provided with additional memory, extra powerful processing facilities or heavy graphics support as required. This environment can also be applied when restrictive requirements are imposed on data sets security, or when additional privacy measures are required.

For whom
The Virtual Research Workspace is based on non-profit and has target groups at universities affiliated with the VSNU and medical centers affiliated with the NFU. Initiatives and partnerships between universities, academic houses and third parties, both commercial and non-profit, are supported under the specific condition that the university or the academic center is the coordinator of the research.

Customer value
It is a place where researchers have full control over their data and results and the risks of data leakage are minimized. You can log in from an existing (own institution) federated account using multi-factor authentication. To ensure that there is no pollution or misuse of data, the internet cannot be accessed directly from the secure work environment. Working in this environment guarantees that your data remains secure, even if your laptop is lost or stolen. The federated account allows you to work safely on several studies at once. Each study has its own closed system, making any direct exchange of data between the studies impossible. The default application landscape is extensive, but specific applications can be incorporated if desired. It is possible to run various versions of the same application simultaneously. All of the virtual workspace components are scalable in capacity if the basic or premium versions do not fulfill your needs. The integrity of the data and results is carefully monitored within the study. For this purpose, various roles are available for each study. A highly secured collaborative environment, role-based, specifically targeted at researchers who work with sensitive data. Great for researchers whose standard university workplace is insufficient and whose applications are not suitable for Linux HPC usage.

What do we offer?
The Virtual Research Workspace (A Windows 10 virtual workspace environment): A reliable, innovative and fast data analysis environment that considerably lightens the burden of work for researchers. Information can be found at http://www.rug.nl/vrw and http://www.rug.nl/rwp.

Usage
Various research initiatives, studies and collaborations within the UG and the UMCG are using this service. RWS enables innovative, collaborative ICT environment while complying to data regulations.

Service owner
Team R & D Workspaces; Teamlead Rinse Posthuma, email r.posthuma@rug.nl
**Security & privacy**

Information security management is set up as a continuous process of planning and monitoring cycles (plan, do, check, act, PDCA), based on ISO27001. It is within these cycles that plans are drawn up and implemented. The results are evaluated and translated into new plans. Over time, processes and systems can change, but also the environment in which these systems operate, the threat landscape, and policies, guidelines and regulations are subject to change. Because of this, the PDCA-cycle is executed annually. Reference: ‘Regulation annual information security and data protection plan. 20 March 2019’

The following security and privacy measures are in place for the VRW:

- Zoning and isolation backend services & network. The virtual research workspace resides in a very trusted zone (baseline information security 2018-4.pdf). By default no direct inbound or outbound traffic will be allowed. No direct internet access.
- Multifactor authentication.
- Federated identity management; login and password management lies within the users own institution.
- All data access is monitored and audited.
- Compliant to the GDPR privacy policy
- Compliant to the Baseline Information Security 2018
- Role based access for layered authorisation.

<table>
<thead>
<tr>
<th>Defined Research Roles</th>
<th>Drive</th>
<th>Data Transfer within VRW</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H: (Home drive)</td>
<td>G: (Group drive)</td>
</tr>
<tr>
<td><strong>Controller</strong></td>
<td>R/W</td>
<td>R/W</td>
</tr>
<tr>
<td><strong>Data Manager</strong></td>
<td>R/W</td>
<td>R/W</td>
</tr>
<tr>
<td><strong>Researcher+</strong></td>
<td>R/W</td>
<td>R/W</td>
</tr>
<tr>
<td><strong>Researcher</strong></td>
<td>R/W</td>
<td>R/W</td>
</tr>
<tr>
<td><strong>Reviewer</strong></td>
<td>R/W</td>
<td>R</td>
</tr>
</tbody>
</table>

**Storage & backup**

By default every user will have a 1 GB homedrive and collaborative groupdrive of 100 GB these drives will be backed-up conform Service level Agreement (Appendix 1). Additional storage can be added on demand. A fair use policy is in effect in regard to overuse.

**Account administration**

**Application**

Account & group registration will be handled by the RDO (RUG). Users of the University of Groningen contact RDO of the University of Groningen: e-mail researchdata@rug.nl or go to https://www.rug.nl/society-business/centre-for-information-technology/research/organisation/contact-form
All requests will be registered in Topdesk and will be followed up with a personal intake if deemed necessary. Minimal information required per user:

- name study
- owner of the study (responsible for study and first contact)
- email (connected to the institutional account if applicable)
- first name
- last name
- mobile phone
- role
- projectcode (finance)
- start date
- Type of workspace (Basic or Premium)

Users will be notified automatically by email when the account is activated and ready for use.

**Data transport**

For secure data transport into the VRW multiple options are available. Data Managers are allowed to upload and download datasets directly into the VRW. We recommend this usage for smaller datasets only. For larger files there is a SFTP environment available within a DMZ.

**Desktop applications**

Application installation requests are based on a fair use policy. For application requests which are highly time consuming a one time fee and/or a custom quotation can be applicable. The VRW has a default set of applications available which are free of use and/or licensed for employees and students of the University of Groningen. For users outside the University of Groningen additional license fees and or usage costs may apply.

**System management**

The basic infrastructure workspaces is hosted, maintained and managed by the CIT. Specifically:

- Network infrastructure
- System hardware
- Virtualisation services (ESX & Citrix)
- Server and Desktop OS
- Middleware (e.g. Database management, IAM)
- Workspace management
- User management (Data)
- Application delivery services

The CIT provides the infrastructure for this system, consisting of hosting the virtual research workspace environment on (virtual) hardware of the RUG. In addition, the CIT ensures:

- technical system management, including incident and change management of the operating system and database, security and keeping the operating system of the system up to date, monitoring of the system, data storage and back-up of the data of the application systems.
- linking to the data storage system (SAN) and back-up system of the CIT and allocating the required storage space.
- the conclusion of a processing agreement between the University of Groningen and external parties, in the context of the General Data Protection Act (AVG).
- communication and consultation with the customer of the system in the event of malfunctions and incidents.
**Support**
The following support desks are available for incidents, disruptions, information and feature requests:

**Support CIT Incidents and disruptions:**
CIT Service Desk, tel. 050-363 3232, e-mail citservicedesk@rug.nl
Outside Office hours in an emergency: Central Emergency Room RUG: Tel. 050-363 5520

**Support RUG RDO:**
Users of the University of Groningen contact RDO of the University of Groningen with questions, incidents and disruptions e-mail researchdata@rug.nl or go to https://www.rug.nl/society-business/centre-for-information-technology/research/organisation/contact-form

**Configuration & Performance**
Two standard configurations are made available:

- **Basic***: The standard configuration is a highly available virtual workspace with 1 GB home drive, 100 GB Group drive. Cpu, Gpu and Memory are shared, so that a performance guarantee can be issued to a lesser extent, but at a level that is powerful at all times. Most suitable for regular research, where no high demands are placed on performance.
- **Premium**: The standard configuration is a highly available virtual workspace with 1 GB home drive, 100 GB Group drive, 2 CPUs, (indication) 1 GB vGPU and 7 GB memory that is guaranteed at all times. Most suitable for advanced research, where high demands are made on performance and / or functionalities.

Customization is possible. Based on a personal intake, a quote can be given for desired capacity and performance.

*A fair use policy is assumed, which can cause performance to fluctuate. This is closely monitored. If the fair use policy is exceeded, resulting in a heavy performance degradation of the systems, measures will be taken against the user concerned. Time penalties can be applied in the performance to protect the integrity of the entire research environment.

**Finance**

**Pricing***

- Basic: €300,- user/year
- Premium: €750,- user/year

Monthly billing based on prepayment.

*Prices are excl. VAT. Service, pricing and terms of usage will be reviewed on an annual basis.

In addition to the costs for the Virtual Research Workspace, which is based on prices negotiated by the University of Groningen, other prices** might apply for other universities and medical centers (possibly combined with commercial parties). Agreements are made with all parties and recorded within an addendum on the generic Service Agreement or DVO for the VRW. A KPI is a standard part of this agreement.
**Additional (external use) license fees and/or special requests during intake such as applications and databases**

**Duration**
This service can be purchased with a minimum duration of one year per user per study/research. A free trial of 2 months with a maximum of 5 users is available. After 2 months the service is automatically converted into an annual subscription, effective on the free trial expiration date, unless the user decides otherwise before the end of the trial period.

**Termination**
The notice period of the VRW is no later than 1 month before the start of the new annual term. You can cancel your subscription by sending an e-mail to researchdata@rug.nl, stating the user group, name(s) and date of termination.

**Connected services**
The following services can be used in conjunction or separate from the VRW but are by default excluded from this agreement. Different terms of usage may be in effect.

- Secure file transfer (SFTP) services
- Secure User Databases
- Data Clearing House, *data linking, pseudonimisation & anonymisation*
- Clinical Trial Processor (CTP), *a service for de-identifying and submitting imaging data.*
- High Performance Cluster (HPC) Services
## Appendix 1 Servicelevels

<table>
<thead>
<tr>
<th>Standaard Servicelevels:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Levertijd diensten</strong></td>
</tr>
<tr>
<td>- Systemen worden opgeleverd op basis van afspraken in een offerte of DVO.</td>
</tr>
<tr>
<td>- Levering gaat in na ondertekening van offerte.</td>
</tr>
<tr>
<td><strong>Beschikbaarheid</strong></td>
</tr>
<tr>
<td>- Het CIT kent GEEN 24/7 dienstverlening. Systemen worden via tools wel 24/7 gemonitord, echter buiten kantooruren zullen alameringen o.b.v. best effort worden opgepakt.</td>
</tr>
<tr>
<td>- De beheerders zijn beschikbaar tijdens kantooruren (08.30 – 17.00 uur, CET). Omtrent werkzaamheden buiten kantooruren kunnen in overleg aanvullende afspraken worden gemaakt die in de dienstverleningsovereenkomst worden opgenomen.</td>
</tr>
<tr>
<td>- 7 dagen per week beschikbaar, binnen kantoor tijd wordt gestreefd naar een beschikbaarheid van 99,9%, daarbuiten 99%, uitgezonderd de diensten die de RUG afneemt van externe partijen die hun eigen service levels hebben voor de beschikbaarheid (bijvoorbeeld Nestor). Zie ook onderhoud.</td>
</tr>
<tr>
<td>- De afgesproken servicelevels treden buiten werking in het geval van calamiteiten.</td>
</tr>
<tr>
<td><strong>Kortdurend Onderhoud</strong></td>
</tr>
<tr>
<td>- Maandag en woensdag van 06.00-08.00 uur voor kort, onaangekondigd onderhoud, uitgezonderd de onderhoudsvensters die door externe partijen worden gehanteerd. (Voorbeeld Nestor)</td>
</tr>
<tr>
<td><strong>Groot onderhoud of wijzigingen</strong></td>
</tr>
<tr>
<td>- Groot onderhoud of wijzigingen van de dienst geschieden via de changeprocedures van het CIT en worden minimaal 5 werkdagen van tevoren per mail aangekondigd bij de contactpersoon van de opdrachtgever.</td>
</tr>
<tr>
<td>- Wijzigingsverzoeken tijdens de operationele fase aan de systemen van de Opdrachtgever in onderling overleg tussen de Contactpersoon van de Opdrachtgever en het CIT nader uitgewerkt, ingepland en doorgevoerd. Dit betreft ook verzoeken tot installatie van extra/nieuwe applicaties en updates van applicaties.</td>
</tr>
<tr>
<td>- Indien aan een voorgestelde wijziging extra kosten zijn verbonden, ontvangt de Opdrachtgever hiervoor een aanvullende offerte van het CIT.</td>
</tr>
<tr>
<td>- Wijzigingen, mits niet van grote impact, hebben een doorlooptijd voor het uitvoeren hiervan, van niet meer dan 5 werkdagen nadat het besluit tot doorvoeren van de wijziging is genomen.</td>
</tr>
<tr>
<td>- Grote updates (versiewijzigingen) en aanpassingen worden opgenomen in het changemanagement van het CIT. Hierin wordt in overleg met de opdrachtgever o.a. een planning vastgesteld voor het uitvoeren van de wijziging.</td>
</tr>
<tr>
<td>- In geval van een “urgent change” zal de uitvoering in overleg met de opdrachtgever worden vastgesteld.</td>
</tr>
<tr>
<td><strong>Ondersteuning, incidentmeldingen, vragen en verzoeken</strong></td>
</tr>
<tr>
<td>- Incidenten en vragen kunnen op maandag t/m vrijdag van 8.30-17.00 worden gemeld bij de servicedesk van het CIT.</td>
</tr>
<tr>
<td><strong>Storingslevel</strong></td>
</tr>
<tr>
<td>- Het CIT hanteert het volgende service level:</td>
</tr>
<tr>
<td>- Reactietijd: Binnen 4 uur (op werkdagen tussen 08.30 en 17.00 uur) na melding of constatering van het incident of verstoring; Correctieve actie (op werkdagen tussen 08.30 en 17.00 uur) binnen 4 uur na constatering of melding van de verstoring.</td>
</tr>
<tr>
<td>- buiten kantooruren: op basis van best effort, in overleg en conform afspraken in de dienstverleningsovereenkomst.</td>
</tr>
<tr>
<td>- In geval van storing, langer dan 4 uren, van systemen van de opdrachtgever of systemen van de RUG die de opdrachtgever raken, waarvan de impact hoog is, treedt de calamiteitenprocedure in werking.</td>
</tr>
<tr>
<td><strong>Communicatie bij storingen en Calamiteiten</strong></td>
</tr>
</tbody>
</table>
| - Bij calamiteiten neemt een vertegenwoordiger van het CIT calamiteitenteam zo spoedig als mogelijk (streven binnen 4 werken)
nadat het calamiteitenteam bijeen is gekomen) contact op met de contactpersonen van de Opdrachtgever.

| Rapportages | ● Per kwartaal rapportage over calamiteiten, (bijna) verstoringen en datalekken.  
|             | ● Eventuele aanvullende afspraken over te rapporteren zaken van verschillende (specifieke) diensten zijn vermeld in de betreffende dienstbeschrijvingen. |
| Back-up en restore | Het CIT voert de volgende standaard parameters voor haar back-up dienst:  
|                 | ● Maximale dataloss tijd is 24 uur.  
|                 | ● Maximale bewaartijd van gedelete files is 30 dagen.  
|                 | ● Om de files te restoren is het niet nodig alle incremental back-ups terug te zetten.  
|                 | ● Restore van files kan zowel op directory- als file-niveau gebeuren. Daarbij kan de laatste versie of een eerdere versie worden teruggezet. Tevens is een 'point in time'-restore mogelijk, b.v. van een complete directory.  
|                 | ● Het terugzetten van verwijderde files is mogelijk, mits de bewaartijd niet verstreken is.  
|                 | ● De Opdrachtgever van de dienst kan zelf bepalen wanneer hij de restore wil doen en van welke files. De restore-duur bij een algehele crash is max. 24 uur, tenzij de benodigde infrastructuur buiten werking is. In dat geval is er sprake van een andere verstoring of zelfs calamiteit.  
|                 | ● Aanvragen van file restore dienen te worden ingediend bij de Servicedesk. |

**Appendix 2 Information Security Baseline**

Information Security Baseline: rug_baseline_inf bev v 1.0.pdf