VU VRIJE UNIVERSITEIT AMSTERDAM

Basic Research Data Classification Tool

Export selection: 23/05/2025 06:49:23

Filters

Confidentiality

Nothing selected

Integrity

Nothing selected

Availability

Nothing selected

Selected options

Low risk

No significant risks identified. Follow basic steps for selecting storage.

With no significant risks on the data identified, the next step is selecting a storage and or application that fits the functional needs for your research project.

You can use the Storage Finder as first step for finding the right storage. Select "Low" at "Data classification".

If some specific requirements are not met, please contact theRDM support desk.

More info

Confidentiality:	Low
Integrity:	Low
Availability:	Low

Confidentiality risk Low, risk on Integrity

Some action required regarding choosing the right storage solution. Some mandatory checks.

Follow questions and instructions below.

Additional questions on Integrity

First some additional questions on the exact level of risk regarding Integrity, this helps finding the right (storage) solution(s) for you research project.

Check the three questions below. The highest level found is used as the overall level of risk for Integrity.

- *Specify multiple people with access to the data*

-- Multiple users in project and within VU with read access: Medium

-- Multiple users outside project or outside VU with read access: High

-- User or users outside project with edit access: High

- *Specify impact on research if data is corrupted after collection (and collection can not be done again):*

-- Minimal to none (only ego's hurt): Low

-- Moderate (financial impact, delay in publication): Medium

-- Severe: High

- *Specify impact on research participants if data is corrupted after collection*

-- Data not publicly available and/or data not needed for follow up actions: Medium

-- Otherwise: High

Select storage option

Storage options can be found using the Storage Finder.

Select "Low" at Data Classification (Confidentiality).

If Integrity is critical a solution providing proper access management, monitoring and logging should be selected. Solutions suitable for Data Classification (Confidentiality) High include those items.

It is required to do a full CIA classification (Dutch: BIV classificatie). For bigger research projects or projects with high public profile, it's also required.

Please contact the Security and Privacy Team for requesting a CIA/BIV classification.

No personal data is involved. A DPIA is not required.

Use steps above to further complete the DMP.

More info

Confidentiality:	Low
Integrity:	Medium or High
Availability:	Low

Confidentiality risk Low, risk on Availability

Some action required regarding choosing the right storage solution. Click to read the details.

Please read instructions for next steps and answer the extra questions for your project.

Additional questions on Availability

First some additional questions on the exact level of risk regarding Availability, this helps finding the right (storage) solution(s) for your research project.

Check the three questions below. The highest level found is used as the overall level of risk for Availability.

- How readily do your data need to be available to you or your research team?

-- 7 days a week 24 hour a day: High

-- Frequent, but not 24/7 (for example working hours): Medium

-- Anything less frequent: Low

- How long would data need to be unavailable for your research project to suffer serious harm (i.e. not just minor inconveniences)?

-- Up to one hour: High

-- Up to one day: Medium

-- Up to one week or longer: Low

- How long will the data need to be stored and maintained?

-- Up to 10 years after the last research publication is published: Low

-- Indefinitely: High

Finding storage

Storage options can be found using the Storage Finder.

Select "Low" at Data Classification.

If accessibility is most important, a solution providing good backup and 99.9% uptime should be found

If data loss or long term storage is important, proper backups and a future proof solution should be selected.

Options provided by the VU as shown in Storage Finder are suitable for both aspects, except portable storage, SurfDrive and Google Drive.

If one of the chosen items is of critical importance, please contact the RDM Support Desk for further advice.

Further steps

If one of the risks is High, a full BIV classification done by an ISO is required. Otherwise use the online BIV classification form that can be found here: [linkt to be provided].

For bigger research projects or projects with high public profile, it is recommended to do the BIV together with an ISO.

Please contact the Security and Privacy Team for requesting a BIV classification.

No personal data is involved. A DPIA is not required.

Use steps above to further complete the DMP.

More info

Confidentiality:	Low
Integrity:	Low
Availability:	Medium or High

Confidentiality risk Low, risks on Integrity and Availability

Some action required regarding choosing the right storage solution and some mandatory checks.

Follow questions and instructions below.

Additional questions on Integrity

First some additional questions on the exact level of risk regarding Integrity, this helps finding the right (storage) solution(s) for you research project.

Check the three questions below. The highest level found is used as the overall level of risk for Integrity.

- *Specify multiple people with access to the data*

-- Multiple users in project and within VU with read access: Medium

-- Multiple users outside project or outside VU with read access: High

-- User or users outside project with edit access: High

- *Specify impact on research if data is corrupted after collection (and collection can not be done again):*

-- Minimal to none (only ego's hurt): Low

-- Moderate (financial impact, delay in publication): Medium

-- Severe: High

- *Specify impact on research participants if data is corrupted after collection*

-- Data not publicly available and/or data not needed for follow up actions: Medium

-- Otherwise: High

Additional questions on Availability

First some additional questions on the exact level of risk regarding Availability, this helps finding the right (storage) solution(s) for your research project.

Check the three questions below. The highest level found is used as the overall level of risk for Availability.

- How readily do your data need to be available to you or your research team?

-- 7 days a week 24 hour a day: High

-- Frequent, but not 24/7 (for example working hours): Medium

-- Anything less frequent: Low

- How long would data need to be unavailable for your research project to suffer serious harm (i.e. not just minor inconveniences)?

-- Up to one hour: High

-- Up to one day: Medium

-- Up to one week or longer: Low

- How long will the data need to be stored and maintained?

-- Up to 10 years after the last research publication is published: Low

-- Indefinitely: High

Finding storage

Storage options can be found using the Storage Finder.

Select "Low" at Data Classification (Confidentiality).

If Integrity is critical a solution providing proper access management, monitoring and logging should be selected. Solutions suitable for Data Classification (Confidentiality) High include those items.

If Availability is most important, a solution providing good backup and 99.9% uptime should be found

If data loss or long term storage is important, proper backups and a future proof solution should

be selected.
Options provided by the VU as shown in Storage Finder are suitable for both aspects, except portable storage, SurfDrive and Google Drive.

If one of the chosen items is of critical importance, please contact the RDM Support Desk [LINK] for further advice.

Because of the level of risks already identified it is needed to do a full CIA Classification (Dutch: BIV classificatie). For bigger research projects or projects with high public profile, it's also mandatory..
Please contact the Security and Privacy Team for requesting a CIA/BIV classification.

It is optional to do a full BIV classification. For bigger research projects or projects with high public profile, it's recommended.

No personal data is involved. A DPIA is not required.
Use steps above to further complete the DMP.
More info

Confidentiality:	Low
Integrity:	Medium or High
Availability:	Medium or High

Confidentiality risk Medium

Action required and two mandatory checks apply.

Instructions on further steps

Some of the data is sensitive. Additional steps need to be taken.
A full CIA classification (Dutch: BIV classificatie) is needed in order to assess the details of the risks involved.
Please contact the Security and Privacy Team for requesting a CIA/BIV classification. This can be done online.
There is medium risk on Confidentiality.
You can select a storage option using the Storage Finder. Select "M" at Data Classification - Confidentiality.
A DPIA (Data Protection Impact Assessment) may be legally required when personal data is involved. Please contact with your Privacy Champion.

Use feedback from all steps above to fill the DMP. You can useDMPOnline for this (introduction)
More info

Confidentiality:	Medium
Integrity:	Low
Availability:	Low

Confidentiality risk Medium, risk on Integrity

Some mandatory actions are required.

Instructions on further steps

Additional questions on Integrity

First some additional questions on the exact level of risk regarding Integrity, this helps finding the right (storage) solution(s) for you research project.

Check the three questions below. The highest level found is used as the overall level of risk for Integrity.

- *Specify multiple people with access to the data*

-- Multiple users in project and within VU with read access: Medium

-- Multiple users outside project or outside VU with read access: High

-- User or users outside project with edit access: High

- *Specify impact on research if data is corrupted after collection (and collection can not be done again):*

-- Minimal to none (only ego's hurt): Low

-- Moderate (financial impact, delay in publication): Medium

-- Severe: High

- *Specify impact on research participants if data is corrupted after collection*

-- Data not publicly available and/or data not needed for follow up actions: Medium

-- Otherwise: High

Full classification

Some of the data is sensitive/confidential and there are Integrity risks. It is required to do a full CIA classification (Dutch: BIV classificatie) in order to assess the details of the risks involved. Please contact the Security and Privacy Team for requesting a CIA/BIV classification.

Select storage option

If Integrity is critical (items with "High") a solution providing proper access management, monitoring and logging should be selected. Solutions suitable for Data Classification (Confidentiality) High include those items.

If no personal data is involved, you can select a storage option using theStorage Finder. Select "M" at Data Classification - Confidentiality.

A DPIA (Data Protection Impact Assessment) may be legally required when personal data is involved. Please contact with your Privacy Champion.

Use feedback from all steps above to fill the DMP.

You can use DMPOnline for this (introduction)

More info

Confidentiality:	Medium
Integrity:	Medium or High
Availability:	Low

Confidentiality risk Medium, risk on Availability

Some actions are required. Some mandatory checks are needed.

Please read instructions for next steps and answer the extra questions for your project.

Additional questions

Some additional questions on the exact level of risk regarding Availability, this helps finding the right (storage) solution(s) for your research project.

Check the three questions below. The highest level found is used as the overall level of risk for Availability.

- How readily do your data need to be available to you or your research team?
-- 7 days a week 24 hour a day: High
-- Frequent, but not 24/7 (for example working hours): Medium
-- Anything less frequent: Low
- How long would data need to be unavailable for your research project to suffer serious harm (i.e. not just minor inconveniences)?
-- Up to one hour: High
-- Up to one day: Medium
-- Up to one week or longer: Low
- How long will the data need to be stored and maintained?
-- Up to 10 years after the last research publication is published: Low
-- Indefinitely: High

Finding storage

If no direct identifiable personal data is involved, you can select a storage option using the Storage Finder. Select "M" at Data Classification - Confidentiality.
If accessibility is most important, a solution providing good backup and 99.9% uptime should be found
If data loss or long term storage is important, proper backups and a future proof solution should be selected.
Options provided by the VU as shown in Storage Finder are suitable for both aspects, except portable storage, SurfDrive and Google Drive.

If one of the chosen items is of critical importance, please contact the RDM Support Desk for further advice.

Further steps

Given the level of risk a full CIA Classification (Dutch: BIV classificatie) is needed. Please contact the Security Team for requesting a CIA/BIV classification (online).
For bigger research projects or projects with high public profile, it is recommended to do the CIA/BIV together with an ISO.

A DPIA (Data Protection Impact Assessment) may be legally required when personal data is involved. Please contact with your Privacy Champion.

Use feedback from all steps above to fill the DMP. You can useDMPOnline for this (introduction)

More info

Confidentiality:	Medium
Integrity:	Low
Availability:	Medium or High

Confidentiality risk Medium, risks on Integrity and Availability

Action is required. Some steps are mandatory.

Follow questions and instructions below.

Additional questions on Integrity

First some additional questions on the exact level of risk regarding Integrity, this helps finding the right (storage) solution(s) for you research project.

Check the three questions below. The highest level found is used as the overall level of risk for Integrity.

- *Specify multiple people with access to the data*
-- Multiple users in project and within VU with read access: Medium
-- Multiple users outside project or outside VU with read access: High
-- User or users outside project with edit access: High
- *Specify impact on research if data is corrupted after collection (and collection can not be done again):*
-- Minimal to none (only ego's hurt): Low
-- Moderate (financial impact, delay in publication): Medium
-- Severe: High
- *Specify impact on research participants if data is corrupted after collection*
-- Data not publicly available and/or data not needed for follow up actions: Medium
-- Otherwise: High

Additional questions on Availability

First some additional questions on the exact level of risk regarding Availability, this helps finding the right (storage) solution(s) for your research project.

Check the three questions below. The highest level found is used as the overall level of risk for Availability.

- How readily do your data need to be available to you or your research team?
-- 7 days a week 24 hour a day: High
-- Frequent, but not 24/7 (for example working hours): Medium
-- Anything less frequent: Low
- How long would data need to be unavailable for your research project to suffer serious harm (i.e. not just minor inconveniences)?
-- Up to one hour: High
-- Up to one day: Medium
-- Up to one week or longer: Low
- How long will the data need to be stored and maintained?
-- Up to 10 years after the last research publication is published: Low
-- Indefinitely: High

Finding storage

Storage options can be found using the Storage Finder.
Select "Medium" at Data Classification (Confidentiality).

If Integrity is critical a solution providing proper access management, monitoring and logging should be selected. Solutions suitable for Data Classification (Confidentiality) High include those items.

If Availability is most important, a solution providing good backup and 99.9% uptime should be found

If data loss or long term storage is important, proper backups and a future proof solution should be selected.
Options provided by the VU as shown in Storage Finder are suitable for both aspects, except portable storage, SurfDrive and Google Drive.

If one of the chosen items is of critical importance, please contact the RDM Support Desk [LINK] for further advice.

Because of the level of risks already identified it is needed to do a full CIA Classification (Dutch: BIV classificatie). For bigger research projects or projects with high public profile, it's also mandatory..
Please contact the Security Team for requesting a CIA/BIV classification.

A DPIA (Data Protection Impact Assessment) may be legally required when personal data is invovled. Please contact with your Privacy Champion.

Use feedback from all steps above to fill the DMP. You can useDMPOnline for this (introduction)

More info

Confidentiality:	Medium
Integrity:	Medium or High
Availability:	Medium or High

Confidentiality risk High

Mandatory actions, focussed on sensitivity of the data.

Instructions on next steps

Focus should be on finding a secure solution matching the sensitivity of the data. But also to have a meeting with the Privacy Champion and Faculty Data Steward on what non-technical steps can be taken within the research project to ensure safe handling of data.

Finding storage

Storage options can be found using the Storage Finder.
Select "High" at Data Classification (Confidentiality).
Because of the level of risks identified it is needed to do a full CIA Classification (Dutch: BIV classificatie). For bigger research projects or projects with high public profile, it's also mandatory..
Please contact the Security Team for requesting a CIA/BIV classification.

A DPIA (Data Protection Impact Assessment) may be legally required when personal data is invovled. Please contact with your Privacy Champion.

Use feedback from all steps above to fill the DMP. You can useDMPOnline for this (introduction)

More info

Confidentiality:	High
Integrity:	Low
Availability:	Low

Confidentiality risk High, risk on Integrity

Mandatory steps to be taken.

Instructions on next steps

Focus should be on finding a secure solution matching the sensitivity of the data. But also to have a meeting with the Privacy Champion and Faculty Data Steward on what non-technical steps can be taken within the research project to ensure safe handling of data.

Additional questions on Integrity

First some additional questions on the exact level of risk regarding Integrity, this helps finding the right (storage) solution(s) for you research project.

Check the three questions below. The highest level found is used as the overall level of risk for Integrity.

- *Specify multiple people with access to the data*

-- Multiple users in project and within VU with read access: Medium

-- Multiple users outside project or outside VU with read access: High

-- User or users outside project with edit access: High

- *Specify impact on research if data is corrupted after collection (and collection can not be done again):*

-- Minimal to none (only ego's hurt): Low

-- Moderate (financial impact, delay in publication): Medium

-- Severe: High

- *Specify impact on research participants if data is corrupted after collection:*

-- Data not publicly available and/or data not needed for follow up actions: Medium

-- Otherwise: High

Finding storage

Storage options can be found using the Storage Finder.

Select "High" at Data Classification (Confidentiality).

If Integrity is critical a solution providing proper access management, monitoring and logging should be selected. Solutions suitable for Data Classification (Confidentiality) High include those items.

Because of the level of risks identified it is needed to do a full CIA Classification (Dutch: BIV classificatie). For bigger research projects or projects with high public profile, it's also mandatory..

Please contact the Security Team for requesting a CIA/BIV classification.

A DPIA (Data Protection Impact Assessment) may be legally required when personal data is invovled. Please contact with your Privacy Champion.

Use feedback from all steps above to fill the DMP. You can useDMPOnline for this (introduction)

More info

Confidentiality:	High
Integrity:	Medium or High
Availability:	Low

Confidentiality risk High, risk on Availability

Mandatory steps needed, extra attention to Confidentiality.

Instructions on steps to take

Focus should be on finding a secure solution matching the sensitivity of the data. But also to have a meeting with the Privacy Champion and Faculty Data Steward on what non-technical steps can be taken within the research project to ensure safe handling of data.

Additional questions on Availability

First some additional questions on the exact level of risk regarding Availability, this helps finding the right (storage) solution(s) for your research project.

Check the three questions below. The highest level found is used as the overall level of risk for Availability.

- *How readily do your data need to be available to you or your research team?*
-- 7 days a week 24 hour a day: High
-- Frequent, but not 24/7 (for example working hours): Medium
-- Anything less frequent: Low
- *How long would data need to be unavailable for your research project to suffer serious harm (i.e. not just minor inconveniences)?*
-- Up to one hour: High
-- Up to one day: Medium
-- Up to one week or longer: Low
- *How long will the data need to be stored and maintained?*
-- Up to 10 years after the last research publication is published: Low
-- Indefinitely: High

Finding storage

Storage options can be found using the Storage Finder.
Select "High" at Data Classification (Confidentiality).
If Availability is most important, a solution providing good backup and 99.9% uptime should be found
If data loss or long term storage is important, proper backups and a future proof solution should be selected.
Options provided by the VU as shown in Storage Finder are suitable for both aspects, except portable storage, SurfDrive and Google Drive.
If one of the chosen items is of critical importance, please contact the RDM Support Desk [LINK] for further advice.

Because of the level of risks identified it is needed to do a full CIA Classification (Dutch: BIV classificatie). For bigger research projects or projects with high public profile, it's also mandatory.. Please contact the Security Team for requesting a CIA/BIV classification.

A DPIA (Data Protection Impact Assessment) may be legally required when personal data is invovled. Please contact with your Privacy Champion.

Use feedback from all steps above to fill the DMP. You can useDMPOnline for this (introduction)
More info

Confidentiality:	High
Integrity:	Low
Availability:	Medium or High

Confidentiality risk High, risks on Integrity and Availability

High risk project, mandatory steps.

Instructions on steps to take

Additional questions on Integrity

First some additional questions on the exact level of risk regarding Integrity, this helps finding the right (storage) solution(s) for you research project.

Check the three questions below. The highest level found is used as the overall level of risk for Integrity.

- *Specify multiple people with access to the data*

-- Multiple users in project and within VU with read access: Medium

-- Multiple users outside project or outside VU with read access: High

-- User or users outside project with edit access: High

- *Specify impact on research if data is corrupted after collection (and collection can not be done again):*

-- Minimal to none (only ego's hurt): Low

-- Moderate (financial impact, delay in publication): Medium

-- Severe: High

- *Specify impact on research participants if data is corrupted after collection:*

-- Data not publicly available and/or data not needed for follow up actions: Medium

-- Otherwise: High

Additional questions on Availability

First some additional questions on the exact level of risk regarding Availability, this helps finding the right (storage) solution(s) for your research project.

Check the three questions below. The highest level found is used as the overall level of risk for Availability.

- How readily do your data need to be available to you or your research team?

-- 7 days a week 24 hour a day: High

-- Frequent, but not 24/7 (for example working hours): Medium

-- Anything less frequent: Low

- How long would data need to be unavailable for your research project to suffer serious harm (i.e. not just minor inconveniences)?

-- Up to one hour: High

-- Up to one day: Medium

-- Up to one week or longer: Low

- How long will the data need to be stored and maintained?

-- Up to 10 years after the last research publication is published: Low

-- Indefinitely: High

Finding storage

Storage options can be found using the Storage Finder.

Select "High" at Data Classification (Confidentiality).

If Integrity is critical a solution providing proper access management, monitoring and logging should be selected. Solutions suitable for Data Classification (Confidentiality) High include those items.

If Availability is most important, a solution providing good backup and 99.9% uptime should be found

If data loss or long term storage is important, proper backups and a future proof solution should be selected.

Options provided by the VU as shown in Storage Finder are suitable for both aspects, except portable storage, SurfDrive and Google Drive.

If one of the chosen items is of critical importance, please contact the RDM Support Desk [LINK] for further advice.

Because of the level of risks identified it is needed to do a full CIA Classification (Dutch: BIV classificatie). For bigger research projects or projects with high public profile, it's also mandatory.. Please contact the Security Team for requesting a CIA/BIV classification.

A DPIA (Data Protection Impact Assessment) may be legally required when personal data is invovled. Please contact with your Privacy Champion.

Use feedback from all steps above to fill the DMP. You can useDMPOnline for this (introduction)

More info

Confidentiality:	High
Integrity:	Medium or High
Availability:	Medium or High

Highest Confidentiality classification

Get in touch with several departments.

Special case

Examples of data involved:

- Medical files or interviews of famous (Dutch) people
- Medical files on the psychological state of people and/or heredity research
- Medical files with heredity information
- Medical files of detainees
- Criminal records
- Genetic data

This kind of data always needs a careful and specific approach. There are no standard processes or systems fit for purpose.

If you process state secrets you are obliged to contact legal@vu.nl

First step should be to contact your faculty Data Steward to receive advice on previous experience with similar projects within the faculty. And then the legal department within your faculty for further advise.

Because of the high level of risks it is mandatory to do a full CIA Classification (Dutch: BIV classificatie). [*Link to explainer need to be added*]

Please contact the Security Team for requesting a CIA/BIV classification.

A DPIA (Data Protection Impact Assessment) may be legally required when personal data is involved. Please contact with your Privacy Champion.

Next step would be to ask the RDM Support Desk for advice on possible solutions. They might set up a meeting with IT for Research to gather more options.

More info

Confidentiality:	Very High
Integrity / Availability:	Not classified