



Data Classification for Service Project

According to the *Directive on "Information Security at ETH Zurich"*¹ all data of a project needs to be categorized **by the project owner** into one of four different classification levels that are associated with individual levels of protection. An overview of the classification levels can be found at the end of this document.

Project name		Version 1
Project owner		

1. Data classification for this project

Please add all data and the respective classification levels:

Data description	Classification	Comments

2. Data provenance

Please check all applicable boxes:

<input type="checkbox"/> All samples and/or data have been lawfully obtained.
<input type="checkbox"/> Ethical approval has been obtained.
<input type="checkbox"/> No ethical approval is necessary for this project.

¹ RSETHZ 203.25 (<https://rechtssammlung.sp.ethz.ch/Dokumente/203.25.pdf>)

3. Rules of behavior according to classification levels:

Based on the respective classification of the data, the following principles need to be followed:

Public	<ul style="list-style-type: none">• No restrictions.
Internal	<ul style="list-style-type: none">• Data will be accessible only by authorized users.• Data can be shared by email.
(Strictly) Confidential	<ul style="list-style-type: none">• Data will be accessible only by authorized users.• Data is only processed and stored on encrypted devices.• For high performance computing the Leonhard Med secure high performance computing infrastructure² is used.• Data is not shared by email unless encrypted.• Data is transferred using an access-controlled and secure infrastructure, e.g. Globus³.

4. Declaration

- I confirm the classification levels specified above for the different types of data in this project.
- I confirm the data provenance specified above for all samples and/or data delivered to NEXUS in this project.
- I confirm following the rules of behavior specified above.

Date:

Name:

Signature of Project Owner

² RSETHZ 438.1 (<https://rechtssammlung.sp.ethz.ch/Dokumente/438.1.pdf>)

³ <https://www.globus.org/data-transfer>

A. Summary description of classification levels

PUBLIC	Public information is any information that has been approved for publication by the relevant authority.
INTERNAL (ETH only)	Information is classified as “internal” if unauthorised individuals’ becoming aware of it could damage the interests of ETH Zurich. Internal information means information intended for members of ETH Zurich.
CONFIDENTIAL	Information is classified as “confidential” if unauthorised individuals’ becoming aware of it could significantly damage the interests of ETH Zurich. Confidential information is information that is (generally) intended for a specific group of people, function or role (internal at ETH or external) only.
STRICTLY CONFIDENTIAL	Information is classified as “strictly confidential” if unauthorised individuals’ becoming aware of it could severely damage the interests of ETH Zurich. Information is deemed to be strictly confidential if it is intended for a restricted, clearly defined and named group of recipients.

Examples for types of data and their respective classification can be found in Appendix 1 of the directive⁴. Appendix 2 provides a comprehensive list of behavior rules.

⁴ RSETHZ 203.25 (<https://rechtssammlung.sp.ethz.ch/Dokumente/203.25.pdf>)