UNIVERSITÄT SIEGEN

Official Gazette

Dated **April 20, 2022** **No. 34/2022**

CONTENTS:

Regulations for the Classification of Information at the University of Siegen

Issued April 20, 2022

Issued by: Rector's Office at the University of Siegen
Editorial: Dezernat 3, Adolf-Reichwein-Straße 2 a, 57076 Siegen, Tel. +49 271/740-4813

Regulations for the Classification of Information at the University of Siegen

Issued April 20, 2022

The translations provide a service to international students, researchers and staff. The legally binding version of the notifications are available in German only.

Definitions, Abbreviations, Cross-References

Term	Definition
BDSG	*Bundesdatenschutzgesetz*
BISB	*Bereichs-Informationssicherheitsbeauftragte*
CD	Compact Disc
CISO	Chief Information Security Officer
DIN	*Deutsches Institut für Normung*
DVD	Digital Versatile Disc
EU-DSGVO	*Datenschutzgrundverordnung der Europäischen Union*
ISO	International Organization for Standardization
NDA	Non-Disclosure Agreement
USB	Universal Serial Bus
ZIMT	Center for Information and Media Technology

RACI Matrix

Recipient	Organizational Unit	RACI
Rector	University of Siegen	A
Chancellor	University of Siegen	A
CISO	University of Siegen	R
Director of Executive Department for Data Protection	University of Siegen	C
ZIMT Management	University of Siegen	C
BISB	University of Siegen	C
All members of the university community	University of Siegen	I

Table 1: RACI Matrix[1]

Associated Documents

Document Name	Storage Location
ISO/IEC 27001:2013	https://www.iso.org/isoiec-27001-information-security.html
BDSG (valid from May 25, 2018)	https://www.gesetze-im-internet.de/bdsg_2018/
EU-GDPR (valid from May 25, 2018)	https://eu-datenschutz.org/
Leitlinie zur Informationssicherheit der Universität Siegen from November 16, 2020	Amtliche Mitteilungen Universität Siegen No. 83/2020

1 **Responsible—**Bears responsibility for the concrete execution (**operational responsibility**). The person who initiates execution (by others) or who performs the activity on their own.
Accountable—Bears accountability in sense of "approve," "endorse," and "sign" (**budgetary responsibility**). The person who bears responsibility in a legal or commercial sense.
Consulted—(**Technical responsibility**). A person whose **expert insight** is obtained. Interpreted as bearing responsibility from a technical standpoint.
Informed—To be informed (right to information)

Richtlinie über die Aufbewahrung, Aussonderung, Archivierung und Vernichtung von Unterlagen an der Universität Siegen dated March 6, 2019	Amtliche Mitteilungen Universität Siegen No. 14/2019

Contents

1 Preamble

Information and ideas are the key to business success. It is thus essential to safeguard information and limit access exclusively to authorized parties.

2 Purpose of the Document

This document provides guidelines for the classification of information into predetermined confidentiality levels; the labeling and handling of information classified as confidential; and the disposal and/or destruction of said information.

3 Scope

These guidelines apply to all organizational units at the University of Siegen (faculties, central university administration, university library, as well as other academic and service units), for the entire IT infrastructure (including IT systems and services operated within those units), and for all members, associates, and guests to the University of Siegen.

All previous regulations regarding the classification of information, data, documents, etc., are rendered invalid and replaced in full by these guidelines. Any internal regulations deviating from these guidelines may only be continued in consultation with and with the written consent of the CISO.

Insofar as specific legal ordinances exist regarding access to information, disclosure, and provision of viewing access to files, such ordinances take precedence over these guidelines.

4 Legal Basis

The obligation to data protection is derived, directly or indirectly, from a variety of legal regulations and ordinances. The EU GDPR and German Federal Data Protection Act are two examples of this.

5 IT Security

5.1 Types of Information and Levels of Confidentiality

Information of all kinds, such as documents, images, drawings, data, and programming on paper or magnetic, electronic, optical, or other data storage media, is to be protected uniformly regardless of its specific form of appearance. One crucial factor in successful preservation of confidentiality is a clear, gradated, and unambiguous system for the categorization and classification of information.

The University of Siegen has established the following four levels of confidentiality for information:

- **“ÖFFENTLICH / PUBLIC”**
- **“NICHT-ÖFFENTLICH / NOT PUBLIC”**
- **“VERTRAULICH / RESTRICTED”**
- **“STRENG VERTRAULICH / CONFIDENTIAL”**

5.2 Categorization of Information

Information and documents are to be categorized by confidentiality level based on the standards defined by the Chief Information Security Officer (CISO). The respective information owner, as the responsible party, is tasked with categorizing information into one of the four available categories.

Information should always be uniformly categorized by confidentiality level, regardless of its specific form of appearance (i.e., in paper form, digital, conceptually, orally, etc.).

5.2.1 "ÖFFENTLICH / PUBLIC"

The "ÖFFENTLICH / PUBLIC" classification is reserved for information intended specifically for publication. Permission and release must be received in advance from the university administration or other authorized persons. This serves to protect the University of Siegen against unintended publication of information and potential related damages to the University of Siegen.

Excepted from this regulation is information that is already publicly known, or which is subject to a publication obligation.

A binding list of authorized persons and types of information that can be released are included in ***Annex 2***.

5.2.1.1 Examples of Information Classified as "ÖFFENTLICH / PUBLIC"

- Information on courses or university events open to the public
- Information about and content from public events
- Information already publicly available on the internet
- Publications from the press office
- Promotional materials
- Items from the Official Gazette
- Doctoral Dissertations
- Organizational charts (insofar as these are not linked to specific persons)

5.2.1.2 Labeling of Information Classified as "ÖFFENTLICH / PUBLIC"

Documents categorized as "ÖFFENTLICH / PUBLIC" and which are intended for open use should contain a note of either "ÖFFENTLICH" or "ÖFFENTLICH / PUBLIC" on their title page. On all additional pages of the document, the note "ÖFFENTLICH" or "ÖFFENTLICH / PUBLIC" should be added in the footer.

Electronic information and files, where possible at a technical level, should also include the note "OEF" in their file name. All written materials that are, by their very nature, intended for publication do not require special labeling, especially public websites. The affiliation with the University of Siegen must be clearly visible for the reader (such as through use of a logo).

5.2.1.3 Distribution of Information Classified as "ÖFFENTLICH / PUBLIC"

This information may be made accessible to the public. No special measures are required, regardless of whether distributed in paper form, electronically, or by voice communication.

5.2.1.4 Sending of Information Classified as "ÖFFENTLICH / PUBLIC"

When sent using the University of Siegen's internal mail system, no sealed outer envelope is required; when being sent outside the university, an envelope with the correct address, but no other special labeling, is required.

Transmission via fax and email is permitted.

Transmission by voice communication (in person or by telephone) is permitted.

5.2.1.5 Retention of Information Classified as "ÖFFENTLICH / PUBLIC"

No special measures or retention requirements apply for documents in paper form or information in electronic form.

5.2.1.6 Disposal of Information Classified as “ÖFFENTLICH / PUBLIC”

Documents in paper form can be disposed of via normal paper recycling. Files in

electronic form can simply be deleted.

5.2.2 “NICHT-ÖFFENTLICH / NONPUBLIC” (without Labeling)

Information intended solely for internal use does not require explicit labeling as such.

Information categorized as “NICHT-ÖFFENTLICH / NONPUBLIC” involves information whose distribution could potentially damage the University of Siegen.

5.2.2.1 Examples of Information Classified as “NICHT-ÖFFENTLICH / NONPUBLIC”

- Project files that do not contain information categorized as “VERTRAULICH / RESTRICTED” or “STRENG VERTRAULICH / CONFIDENTIAL” (see 5.2.3 and 5.2.4)
- Scientific data that cannot be interpreted by third parties and for which no non-disclosure agreements are in place
- In general, plans for the allocation of duties
- Instructions for daily operations, internal guidelines and memorandums, internal reports
- Internal correspondence (emails, chats, etc.) that does not contain information categorized as “VERTRAULICH / RESTRICTED” or “STRENG VERTRAULICH / CONFIDENTIAL” (see 5.2.3 and 5.2.4)

5.2.2.2 Labeling of Information Classified as “NICHT-ÖFFENTLICH / NONPUBLIC”

Information classified as “NICHT-ÖFFENTLICH / NONPUBLIC” does not require explicit labeling. However, it must be clear to all readers that the relevant document originated from the University of Siegen. The title page can contain the note “NICHT-ÖFFENTLICH” or “NICHT-ÖFFENTLICH / NONPUBLIC.” In this case, the note “NICHT-ÖFFENTLICH” or “NICHT-ÖFFENTLICH / NONPUBLIC” is to also be added to the footer of all following pages of the document.

Electronic information and files, where possible at a technical level, can also include the note “NOE” in their file name.

5.2.2.3 Distribution of Information Classified as “NICHT-ÖFFENTLICH / NONPUBLIC”

This information may only be distributed within the University of Siegen. Any disclosure to external parties requires the approval of the responsible member of senior management, to be provided on a case-by-case or task-by-task basis. This approval requirement does not apply if a Non-Disclosure Agreement (NDA) has already been signed with the external recipient.

Prior to disclosure to external parties and regardless of the aforementioned regulations, any information classified as “NICHT-ÖFFENTLICH / NONPUBLIC” must always contain a note to indicate to the recipient that the information is internal and proprietary to the university and as such must a) be handled as confidential, and b) may not be disclosed to third parties. A similar process is to be used for information transmitted via voice communication. The recipient must be explicitly informed that the information is internal to the university and as such must a) be handled as confidential, and b) may not be disclosed to third parties.

5.2.2.4 Sending of Information Classified as “NICHT-ÖFFENTLICH / NONPUBLIC”

When sent using the University of Siegen’s internal mail system, no sealed outer envelope is required; when being sent outside the university, an envelope with the correct address, but no other special labeling, is required.

Transmission via fax and email is permitted.

Transmission by voice communication (in person, by phone) is permitted.

5.2.2.5 Retention of Information Classified as “NICHT-ÖFFENTLICH / NONPUBLIC”

Within the University of Siegen, no special measures are required. When documents with this classification are taken outside university premises, care must be taken that no unauthorized third parties gain access to this information. Storage media containing information categorized as “NICHT-ÖFFENTLICH / NONPUBLIC” must be encrypted. The same applies to mobile devices (smartphones, tablets, laptops).

5.2.2.6 Disposal of Information Classified as “NICHT-ÖFFENTLICH / NONPUBLIC”

Documents in paper form are to be destroyed using a file shredder or confidential waste bin rated to the corresponding security level (see 5.3).

Data in electronic form are to be deleted using a secure deletion process.

5.2.3 “VERTRAULICH / RESTRICTED”

Information is classified as restricted if its distribution would cause damage to the property and/or reputation of the University of Siegen, or if such distribution could have legal consequences.

5.2.3.1 Examples of Information Classified as “VERTRAULICH / RESTRICTED”

- Draft agreements and contracts (framework agreements, research contracts, etc.)
- Concepts and layout documents (safety measures, network plans, etc.)
- Media data and software, developed in-house, from concluded projects
- Examination data (list of grades, test protocol, etc.)
- In general: personal data
- Final reports (inspection reports, audit reports, etc.)
- Confidential contents of committee meetings
- Financial data (budget, etc.)
- Cost accounting for externally funded projects sponsored by the private sector

5.2.3.2 Labeling of Information Classified as “VERTRAULICH / RESTRICTED”

For documents, the note “VERTRAULICH” or “VERTRAULICH / RESTRICTED” must be clearly visible on the title page. A “VERTRAULICH” or “VERTRAULICH / RESTRICTED” note is also to be added to the footer of each page. Furthermore, the note “COPY FORBIDDEN/KOPIEREN VERBOTEN” should be applied to the title page.

Where possible, the confidentiality should be limited to a specific time frame, such as through a stamp on the title page “VERTRAULICH BIS DD.MM.YYYY” or “RESTRICTED UNTIL DD MMM YYYY.” A note must be included to indicate the document’s categorization after that date, such as “after this date, the document is intended only for non-public use.”

Electronic information and files, where possible at a technical level, should also include the note “VTR” in their file name.

5.2.3.3 Distribution of Information Classified as “VERTRAULICH / RESTRICTED”

This information may only be disclosed within the University of Siegen to employees who require the information as part of their duties (need-to-know principle). Any disclosure to external parties requires the prior approval of the responsible member of senior manager, and the recipient must sign an NDA (Non-Disclosure Agreement).

To monitor distribution, a distribution chart must be generated, routinely reviewed, and kept updated.

5.2.3.4 Sending of Information Classified as “VERTRAULICH / RESTRICTED”

When sent using the University of Siegen's internal post system, a sealed envelope with the recipient's correct address is to be used. This envelope must be opaque and sealed (such as through adhesives) such that it cannot be opened unnoticed.

When being sent externally, an envelope with the proper address, but no other special labeling, is to be used. Where possible, registered mail (with return slip) should be used.

Electronic transmission to external parties is only permissible in encrypted form, i.e., via email or using a secure transmission platform. A state-of-the-art encryption process should be used for this. Internal communications at the University of Siegen are encrypted by default.

Disclosure via voice communication may only be performed in person and in the exclusive presence of those persons recorded in the distribution list. In the event of a telephone or other telecommunications-based disclosure, the sharing party must ensure that no authorized persons are present on the recipient side. The sender can achieve this by actively denoting the point after which sensitive information will be discussed and confirming that only those persons recorded on the distribution list are present on recipient’s side. Transfer in a public space (such as a train, airplane, café, or restaurant) is not permitted, as it cannot be ensured that no unauthorized third party is eavesdropping.

5.2.3.5 Retention of Information Classified as “VERTRAULICH / RESTRICTED”

Information classified as “VERTRAULICH / RESTRICTED” must be kept permanently under lock and key. For information stored on IT systems, an additional layer of protection through access controls or encryption is required. Documents may only be transported outside university premises under heightened care. Storage media containing information categorized as “VERTRAULICH / RESTRICTED” must be encrypted. The same applies to mobile devices (smartphones, tablets, laptops).

5.2.3.6 Disposal of Information Classified as “VERTRAULICH / RESTRICTED”

Documents in paper form are to be destroyed using a file shredder or confidential waste bin rated to the corresponding security level (see 5.3).

Data in electronic form is to be deleted using a secure deletion process.

5.2.4 “STRENG VERTRAULICH / CONFIDENTIAL”

Information is classified as confidential if its public release would threaten vital interests of the University of Siegen, such as through grievous damages to the property and/or image of the University of Siegen or if such release could incur massive legal consequences.

Information classified in the past as “Secret” remains subject to the same rules. The “Secret” classification is no longer to be used for information. The classification “STRENG VERTRAULICH / CONFIDENTIAL” should instead be used,
including upon update of older information.

5.2.4.1 Examples of Information Classified as “STRENG VERTRAULICH / CONFIDENTIAL”

- Information about existing security measures (configuration of security infrastructure, key distribution plan, etc.)
- Information on grievous vulnerabilities (software, access control, etc.)
- Strategy papers prior to publication
- Data classified as personal and requiring special protection by the GDPR (health data, religious affiliation, etc.)
- Special scientific data (patent documents prior to publication)

5.2.4.2 Labeling of Information Classified as “STRENG VERTRAULICH / CONFIDENTIAL”

The note “STRENG VERTRAULICH / CONFIDENTIAL” must be clearly visible on the title page. The note “STRENG VERTRAULICH / CONFIDENTIAL” must also be added on the footer of each page. Beyond this, the note “COPYING WILL LEAD AUTOMATICALLY TO LEGAL CONSEQUENCES AND IS FORMALLY FORBIDDEN” and/or “KOPIEREN FÜHRT AUTOMATISCH ZU RECHTLICHEN KONSEQUENZEN UND IST AUSDRÜCKLICH VERBOTEN” must also be added to the title page.

Where possible, this restricted status should be limited to a specific time frame, such as through a stamp on the title page “STRENG VERTRAULICH BIS DD.MM.YYYY” or “STRICTLY CONFIDENTIAL UNTIL DD MMM YYYY.” A note must be included to indicate the new categorization after that date, such as “after this date, the document is intended only for nonpublic use.”

Electronic information and files, where possible at a technical level, should also include the note “SVT” in their file name.

5.2.4.3 Distribution of Information Classified as “STRENG VERTRAULICH / CONFIDENTIAL”

This information is only to be made accessible to a highly limited circle of specifically enumerated readers. Any sharing with external parties requires the approval of university management or their vicarious agents**,** and the recipient must sign an NDA (Non-Disclosure Agreement). To monitor distribution, a distribution chart must be generated, routinely reviewed, and kept updated.

5.2.4.4 Sending of Information Classified as “STRENG VERTRAULICH / CONFIDENTIAL”

Personal transfer is the best option for delivering documents at this classification level. Any delivery agent must be personally known and considered trustworthy by the sender. The receipt and handover of documents must always be acknowledged.

In exceptional cases, the sender can forgo the ‘acknowledgment of receipt’ requirement, such as when the documents are personally handed over by sender to receiver, or when trusted aids to the sender such as a person assistant are used for transport.

When sent within the University of Siegen's internal post system, documents must be placed in a closed, opaque envelope sealed against unauthorized opening. A seal in this case can be a stamp or initials on the envelope’s seal or the applicable of non-removable adhesive strips. In addition, the envelope must be personally addressed and appended with the note “persönlich” or “personal.”

For external dispatch, no special label is required for the envelope, although the note “In-person delivery only” should be used. Documents at this classification level may only be sent by registered mail with return slip.

Special care must be taken that the address is correct when sending via external service, and the recipient must review that the envelope has not been tampered with.

Transmission by fax or email is only permissible with prior approval by the responsible member of senior manager. Any such transmission must always be undertaken with encryption, regardless of whether internally or externally. A state-of-the-art encryption process should be used for this.

Transfer via voice communication may only be handled face-to-face and in the exclusive presence of those persons recorded on the distribution list. Phone or other telecommunications transfer, or transfer in a public space (such as a train, airplane, café, or restaurant) is not permitted, as it cannot be ensured that no unauthorized third party is eavesdropping. In any case, the sender must take careful care that no unauthorized persons have an opportunity to eavesdrop on the conversation.

5.2.4.5 Retention of Information Classified as “STRENG VERTRAULICH / CONFIDENTIAL”

Documents at this classification level are to be kept permanently and securely under lock and key (preferably using a safe or comparable security mechanism). For documents stored on IT systems, an additional layer of protection (such as password protection or sharing restrictions) is required beyond the standard access controls and encryption. Documents may be removed from the premises only in extremely unusual circumstances, and then under the utmost of care. Storage media containing information categorized as “STRENG VERTRAULICH / CONFIDENTIAL” must be encrypted. The same applies to mobile devices (smartphones, tablets, laptops).

5.2.4.6 Disposal of Information Classified as “STRENG VERTRAULICH / CONFIDENTIAL”

Documents in paper form are to be destroyed using a file shredder or confidential waste bin rated to the corresponding security level (see 5.3)

Data in electronic form are to be deleted using a secure deletion process.

5.3 Deletion and Disposal of Documents and Storage Media

5.3.1 Disposal of Documents in Paper Form

Paper documents classified as “ÖFFENTLICH / PUBLIC” can be disposed of normally in the appropriate recycling or waste bin.

Paper documents classified as “NICHT-ÖFFENTLICH / NONPUBLIC” are to be disposed of via the provided confidential waste bins or file shredders of at least security rating 2 as per the classifications contained in ISO 21964-1 (DIN 66399).

Paper documents classified as “VERTRAULICH / RESTRICTED" or “STRENG VERTRAULICH / CONFIDENTIAL” are to be disposed of either using a high-quality file shredder classified to at least security rating 5 as per the classifications contained in ISO 21964-1 (DIN 66399) or via special designated confidential waste bins.

The guidelines on the retention, segregation, archiving, and destruction of files at the University of Siegen dated March 6, 2019 (Amtliche Mitteilung 14/2019) must be observed.

5.3.2 Secure Deletion of Storage Media

From both a data protection and IT security standpoint, it must be ensured that sensitive and personal data is securely deleted from storage media, meaning completely and irreversibly (such as through 7x overwrite using WIPE, etc.).

5.3.3 Disposal of Storage Media

Disks, CDs, DVDs, USB sticks, external hard drives, magnetic recording media, storage cards, and other digital storage media must be destroyed using the confidential waste bins provided to us by external service providers. Hard drives are disposed of using a hard drive eraser of category H5 (corresponds to protection class 2 / security level 5 as per DIN 66399) provided by ZIMT.

6 Distribution and Validity

These guidelines enter into effect on the day after their publication. The official German version will be published in the university’s Official Gazette, “Amtliche Mitteilungen der Universität Siegen.”

It contains elements ratified by the Rector’s Office on February 10, 2022.

Siegen, April 20, 2022 Rector

signed

(University Professor Dr. Holger Burckhart)

7 Annexes

7.1 Annex 1: Overview “Rating and Classification of Information”

Classification Level	**“ÖFFENTLICH / PUBLIC”**	**“NICHT-ÖFFENTLICH / NONPUBLIC”**	**“VERTRAULICH / RESTRICTED”**	**“STRENG VERTRAULICH / CONFIDENTIAL”**
Label	**Each page: “ÖFFENTLICH” or “ÖFFENTLICH / PUBLIC”** **In the file name:** **“OEF”**	**Optional on each page:** **“NICHT-ÖFFENTLICH” or “NICHT-ÖFFENTLICH / NONPUBLIC”** **Optional in file names: “NOE”**	**Each page: “VERTRAULICH” or “VERTRAULICH / RESTRICTED”** **In the file name: “VTR”**	**Each page:** **“STRENG VERTRAULICH” or “STRENG VERTRAULICH / CONFIDENTIAL”** **In the file name: “SVT”**
Retention	• No special measures	• Monitored	• **Physical**: Locked in cabinets • Electronically: Password protection	• **Physical**: Preferably in safe/security cabinet • **Electronic**: Encrypted, corresponding user rights concept
Transfer	• No special measures	• No special measures	• **Physical**: In closed, opaque envelope • **Electronic**: Encrypted with modern encryption procedure	• **Physical**: Direct handover or dispatch in closed, opaque, and sealed envelope, check for signs of tampering • **Electronic**: Exclusively encrypted using modern encryption procedure
Retirement and destruction	• No special measures	• **Physical**: Confidential waste bin • **Electronic**: Secured deletion	• **Physical**: Confidential waste bin • **Electronic**: Secured deletion	• **Physical**: File shredded classified as per ISO 21964-1 (DIN 66399) • **Electronic**: Secured deletion (7x wipe or shredding)
Examples	• Information on courses or public university offerings • Information and content from public project	• Files containing no information classified as “VERTRAULICH” or “STRENG VERTRAULICH” (see 5.2.3 and 5.2.4)	• Draft agreements and contracts (framework agreements, research contracts, etc.) • Concepts and layout documents (security	• Information about existing security measures (Configuration of security mechanisms, key distribution plan, etc.) • Information on grievous vulnerabilities

	Events • Information already published on the internet • Publications from the Press Office • Marketing materials • Amtliche Mitteilungen • Doctoral dissertations • Organizational charts (insofar as there are no identified links to specific persons)	• Scientific data that cannot be interpreted by third parties and for which no NDAs are in place • In general, business distribution plans • Instructions on daily operations, internal guidelines and memorandums, internal reports. • Internal correspondence (emails, chat, etc.) not containing information classified as “VERTRAULICH” or “STRENG VERTRAUCH” (see 5.2.3 and 5.2.4).	measures, network plans, etc.) • Media data and proprietary software from completed projects • Examination data (list of grades, test protocol, etc.) • In general, personal data • Final reports (inspection reports, audit reports, etc.) • Sensitive content from committee meetings • Financial data (budget, etc.) • Cost accounting for externally funded projects sponsored by the private sector	(Software, access control, etc.) • Strategy papers prior to publication • Data classified as personal and requiring special protection by the GDPR (health data, religious affiliation, etc.) • Special scientific data (patent documents prior to publication)

7.2 Annex 2: Overview “Persons authorized to release material as “ÖFFENTLICH”

Type of Information	Area	Name	Valid from	Comment
Information on courses	Decentral	Professors /Instructors	April 21, 2022	
Content from public events	Press Office	Director of the Executive Department for Press, Communication and Marketing	April 21, 2022	
Information already published on the internet	Person responsible for homepage	Person responsible for homepage	April 21, 2022	