Bundesministerium
für Wirtschaft
und Klimaschutz

Legally non-binding courtesy translation
(the original version in German language is the only binding one, which needs to be signed)

Code of Practice for the handling of information classified VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) [CLASSIFIED INFORMATION – RESTRICTED] (VS-NfD Code of Practice, non-public bodies/contractors)

concerning version entered into force on 1 September 2023.

Contents

About this Code of Practice on information classified VS-NUR FÜR DEN DIENSTGEBRAUCH: Rights and obligations of the VS-NfD principal and the company

1 VS-NfD contract

Prior to the transmission of information classified VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) to non-public bodies (companies[1]), a contract must be concluded with these bodies which incorporates the provisions of this VS-NfD Code of Practice (Annex 4 to the Manual on the Safeguarding of Classified Information (Geheimschutzhandbuch, GHB)). The specific secrecy requirements of a VS-NfD contract must be clarified between the VS-NfD principal and the VS-NfD contractor. The VS-NfD sub-contractor must also be included in this process (see No. 3.2).

2 VS-NfD principal and VS-NfD originator

For the purposes of this Code of Practice, VS-NfD principals (as contracting authority) are public bodies or companies that must provide companies (VS-NfD contractors) with access to or the possibility to access VS-NfD[2]. For companies, this takes the form of a VS-NfD sub-contract.
The Federal authorities and Federal public-law institutions (government agencies) that prepare VS-NfD or have it prepared, or the legal successor of this government agency, are the VS-NfD originator.

3 Rights and obligations of the VS-NfD principal

3.1 VS-NfD public principal

When passing on VS-NfD to contractors, the VS-NfD public principal must conclude a contract with the company which incorporates the provisions of this Code of Practice (in accordance with 6.6 para. 2 Annex V of the General Administrative Provisions for the Material Protection of Classified Information (Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz – Verschlusssachenanweisung, VSA)). The rights to conduct compliance reviews contained herein are to be exercised in principle by the VS-NfD public principal. Further measures, such as a classified information safeguarding procedure by the Federal Ministry for Economic Affairs and Climate Action (Bundesministerium für Wirtschaft und Klimaschutz, BMWK) or security checks, are not required on VS-NfD classification level.

3.2 VS-NfD non-public principal

If the VS-NfD contractor provides other companies (VS-NfD (sub-)contractor) with access to or the possibility to access to VS-NfD, it is to obligate the VS-NfD sub-contractor to comply with this Code of Practice. In such cases, the prime contractor assumes the role of VS-NfD principal and exercises the corresponding rights to conduct compliance reviews.

[1] The term “non-public body” in the Security Screening Act (Sicherheitsüberprüfungsgesetz, SÜG) primarily includes private-sector companies and institutions under private law. It was adopted as a common term from the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). In the Manual on the Safeguarding of Classified Information (Geheimschutzhandbuch, GHB) and in this Code of Practice, the term “company” is used.
[2] A “classified information contract” only exists for information classified at least VS-VERTRAULICH (CONFIDENTIAL).

4 Obligations of the VS-NfD contractor

4.1 General information

The VS-NfD contractor undertakes to obligate itself comply with the requirements of all parts of this Code of Practice. Express reference is made to possible criminal and contractual consequences in the event of non-compliance.

4.2 Proof of instruction and obligation to comply

Before a person is given access to or the possibility to access VS-NfD, they must be instructed by the company about Part 2 of this Code of Practice and be obligated to comply with it. A copy of Parts 2 and 4 of this Code of Practice is to be made available to them. If the person obtains access to or can gain access to VS-NfD on information technology (IT), the same additionally applies to Part 3 of this Code of Practice. The instruction, obligation to comply and receipt of the required parts of the Code of Practice are to be proven by the person signing the 'Proof of contractor to comply' (VS-NfD Code of Practice Part 5). The proof must be kept by the VS-NfD contractor and must be presented to the VS-NfD principal upon request. The evidence must be destroyed no later than five years after the person concerned has left the activity connected to VS-NfD.

4.3 Control options

The VS-NfD principal is to advise the VS-NfD contractor on the requirements of this Code of Practice and may satisfy itself as to its compliance.

4.4 Designation of a person responsible for information classified VS-NfD

The VS-NfD contractor is to designate a person responsible for compliance with and implementation of the necessary measures for protecting VS-NfD and, if applicable, a deputy, using part 1b) of this sheet.
The VS-NfD principal and the VS-NfD contractor are to each receive a signed copy of Part 1b) of the VS-NfD Code of Practice.

5 Transition period

This Code of Practice (Part 1a), Part 1b), Part 2, Part 3, Part 4, Part 5, Part 6) will enter into force on 1 September 2023. Self-accreditation in accordance with Part 3 of this Code of Practice must be carried out by 1 September 2025.

Agreement on the handling of information classified VS-NUR FÜR DEN DIENSTGEBRAUCH between the VS-NfD principal and the VS-NfD contractor

1. The VS-NfD contractor undertakes to obligate itself with the VS-NfD Code of Practice (Annex 4 to the GHB).

2. In accordance with data protection regulations, the VS-NfD contractor is to designate a person responsible for compliance with and implementation of the necessary measures to protect information classified VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) and, if applicable, a deputy.

   Responsible person (business details):

   Original german version to be filled in only

   ☐ Mr ☐ Ms Surname, Given name:
   Telephone Mobile phone

   Email address Address

   If applicable, representative of the responsible person (business details):

   ☐ Mr ☐ Ms Surname, Given name:
   Telephone Mobile phone

   Email address Address

3. This person is responsible for the following measures, among others, on behalf of the VS-NfD contractor:

- Proof of instruction and obligation of the VS-NfD contractor´s employees who are provided with access to or who can gain access to VS-NfD to comply with the VS-NfD Code of Practice Part 2, Part 3 (if applicable) and Part 4
- Implementation of the requirements of Part 3 of this Code of Practice when processing VS-NfD on IT
- Obtention of the written consent of the VS-NfD principal for the transmission of VS-NfD
- Review of compliance with the necessary measures for protecting VS-NfD at the company, if applicable among VS-NfD sub-contractors as well

Original German version to be signed only.....
.....
[Signature of VS-NfD principal Signature of VS-NfD contractor
Government agency/company: Company:]

General provisions on the handling of information classified VS-NUR FÜR DEN DIENSTGEBRAUCH

1 General remarks

1.1 Applicability

The provisions set out in this VS-NfD Code of Practice apply to German VS-NfD as well as to foreign information with a comparable level of classification that has been passed on to a company in Germany for storage or processing. The same applies to bilateral agreements on the mutual protection of classified information, unless otherwise stipulated therein.
The provisions set out in this VS-NfD Code of Practice do not apply to classified information of supranational or intergovernmental institutions and agencies (such as NATO, EU, ESA, OCCAR) with a comparable level of classification. When protecting such classified information, the respective provisions of these facilities/bodies must be observed.

1.2 'Need-to-know' principle

Only persons who need to have knowledge of a specific VS-NfD in order to perform their duties may obtain knowledge of it. Nobody is to be informed of a specificVS-NfD more fully or earlier than is necessary in order to perform their duties. The principle of knowledge of classified information on a 'need-to-know' basis applies.

1.3 Breaches of confidentiality

Persons who violate the provisions of this VS-NfD Code of Practice may face consequences and criminal punishment for the violation under sections 93 to 99, 203(2) and 353b of the German Criminal Code (StGB).
Persons who have proved unsuitable for handling classified information or whose suitability cannot be assessed are to be precluded from processing VS-NfD by the person responsible for VS-NfD.

1.4 Notification obligations in case of loss of VS-NfD and infringements of the provisions of this VS-NfD Code of Practice

The loss of VS-NfD as well as suspected and detected violations of the provisions of this VS-NfD Code of Practice must be reported immediately to the person responsible for VS-NfD. This person is to immediately inform the VS-NfD principal. Notification obligations of companies subject to confidentiality as per the GHB will remain unaffected. The necessary measures to avert or reduce damage and prevent recurrence are to be taken without delay. The person responsible for VS-NfD must endeavour to clarify the facts.

1.5 VS-NfD on IT

When using IT to handle VS-NfD, Part 3 of this Code of Practice must also be complied with. For the persons processing the data, the requirements for processing under No. 3 are particularly relevant.

2 Classification

The Federal authorities and Federal public-law institutions (government agencies) that prepare VS-NfD or have it prepared, or the legal successor of this government agency, are VS-NfD originators. The originator of VS-NfD classifies information as VS-NfD if its disclosure to

unauthorised persons could be disadvantageous to the interests of the Federal Republic of Germany or one of its federal states (Section 4(2) No. 4 Security Screening Act (Sicherheitsüberprüfungsgesetz, SÜG)). Classification as VS-NfD is only to be used insofar as it is necessary.
The VS-NfD originator determines which information is to be classified. The contractor can only make a classification at the behest of the VS-NfD originator. It always remains the creator of the VS-NfD only and never its originator. The company must ensure the required VS-NfD classification.

3 Termination and declassification

The classification of VS-NfD is limited to 30 years. The VS-NfD originator, taking into account the justification for the classification, may determine a shorter period. The classification finishes at the end of the year in which the end of the period falls. The period cannot be extended.
If VS-NfD is no longer classified, the VS-NfD originator must declassify the classification or arrange for the company to implement this declassification. The declassification of the classification is to be recorded in such a way that its new status and the enacting agency can be identified at all times.

4 Markings

When created, VS-NfD is to be marked in such a way that, when handled, the classification level, the creating entity, the VS-NfD originator, the date of classification and the end of classification as determined by the originator (if less than the standard period of 30 years) are identifiable at all times throughout the period of its classification.
The mandatory design of the marking for VS-NfD can be found in Part 4 of this Code of Practice.
If the nature of the VS-NfD does not permit such marking to be undertaken, it should be handled in an equivalent manner. Classification levels are to be written out, insofar as the nature of the classified material permits such a marking. If this is not possible, the classification level VS-NUR FÜR DEN DIENSTGEBRAUCH is abbreviated to VS-NfD.
In the case of non-German classified information with a comparable level of classification, it is additionally to be marked with the German classification level, inasmuch as this is provided for in the applicable security agreements.

5 Storage

VS-NfD is to be kept in locked containers or rooms when not in use to protect against unauthorised persons gaining knowledge of it (‘need-to-know’ principle). Outside such rooms or containers, it must also be handled in such a way as to prevent unauthorised persons from gaining knowledge of it. If VS-NfD cannot be destroyed or returned in full after the task has been carried out, it must be kept in accordance with the requirements of this Code of Practice until the classification is declassified.
VS-NfD Interim Classified Information (e.g. preliminary drafts) is to be protected in the same way as the reference document.

6 Disclosure/Transmission

Disclosure refers to the handing over or making available of VS-NfD following which another person has access to or can obtain it.

6.1 Necessity

Before each transmission of VS-NfD, it must be assessed whether such transmission is actually necessary in order for the task to be fulfilled based on the 'need-to-know' principle.

6.2 Transmission within a company

VS-NfD can be passed on openly within a company, although in such instances it must also be ensured that unauthorised persons cannot gain knowledge of it. A receipt for this type of transmission is not required.

6.3 Disclosure to third parties (public bodies or companies)

Through the transmission of VS-NfD to a third party, the third party has access to it or can obtain it. Disclosure may also be necessary if a third party is able to gain access through an activity (e.g. maintenance, repair) that is required in order for the task to be performed. In this case, measures are to be taken to prevent access to the classified information (e.g. technical measures, covering, escorting). The transmission of VS-NfD to third parties is only permissible if proof of consent of the VS-NfD originator is obtained prior to transmission. The VS-NfD originator may consent on a case-by-case basis, but may also consent in advance to certain or all transmissions of VS-NfD under one or more
VS-NfD contract and VS-NfD sub-contracts within a particular programme. Consent may also be given for activities where a third party may gain access to VS-NfD during the execution of a contract. This consent must be obtained via the VS-NfD principal. Companies may rely on a written declaration from the relevant VS-NfD principal that such consent has been obtained from the VS-NfD originator. They are to keep the declaration as proof.

6.4 Disclosure to non-German public agencies and companies based abroad

VS-NfD can also be permitted to be disclosed to non-German public agencies (foreign public bodies or supranational or intergovernmental institutions and bodies) and companies[1] based abroad provided that the originator of the classified information has given consent. In addition to the aspects listed above, additional requirements must be observed as follows.
The transmission of German VS-NfD to non-German public agencies requires, in principle, a bilateral governmental or ministerial agreement on the mutual protection of classified information or a corresponding international agreement (agreement on the mutual protection of classified information) that regulates the conditions for its transmission and further handling.
The transmission of VS-NfD to companies based abroad takes place on the basis of contractual agreements and, in principle, on the condition that an agreement on the mutual protection of classified information governing the protection of German VS-NfD has been signed with the recipient country.[2] The agreement on the mutual protection of classified information must be referred to in the contractual agreement.
If there is no bilateral governmental or ministerial agreement on the mutual protection of classified information or a corresponding international agreement, the originator of the classified information must determine the modalities of transmission to non-German public agencies or companies based abroad in consultation with the Federal Ministry for Economic Affairs and Climate Action on a case-by-case basis, in accordance with the VSA.

[1] See part 1a), No. 1.
[2] The Federal Ministry for Economic Affairs and Climate Action must be asked whether an agreement on the mutual protection of classified information exists with the respective recipient country and whether comparability with VS-NfD has been agreed therein.

6.5 Transmission using private delivery services

Information classified VS-NfD can be sent via private delivery services as ordinary letters or parcels. The envelope or the parcel is not to be marked with a label indicating that it contains classified information.

VS-NfD may also be transmitted across borders using private delivery services as described above, unless the specific bilateral agreement on the mutual protection of classified information does not permit transmission in this way or the VS-NfD principal or the VS-NfD originator has objected to such transmission.

7 Taking VS-NfD away from company premises and working from home

VS-NfD can only be taken outside of company premises on business trips and to meetings insofar as this is necessary in order for the task to be fulfilled and it is adequately secured against unauthorised persons gaining knowledge of or access to it. In such cases, VS-NfD, among other documents, may be carried in a closed envelope which does not bear a seal.
It is generally not permitted for VS-NfD to be taken into the home to be processed from there. VS-NfD in electronic form may however be processed from the home under the conditions listed in Part 3, No. 3.5. The public VS-NfD principal may allow further exceptions. VS-NfD sub-contractor may rely on a written declaration from their VS-NfD principal attesting that such an exemption has been allowed. They are to keep the declaration as proof.
In addition to the exemption, the following points must be complied with:

- The private home has to be located within Germany
- The person responsible for VS-NfD has given consent
- The employee has been informed about the specific risks of working from home
- Part 6 of this Code of Practice has been signed by the employee and is retained by the company as proof

8 Destruction

In order to prevent the amassing of large stocks of VS-NfD, VS-NfD that is no longer required must be destroyed or returned to the VS-NfD principal.
VS-NfD, including VS-NfD Interim Classified Information, is to be destroyed by the processing persons in the designated places only and in such a way that the content is neither recognisable nor can be made recognisable.
As a matter of principle, only products, processes or service providers that meet the requirements of the Federal Office for Information Security (Bundesamt für Sicherheit und Informationstechnik, BSI) may be used for the destruction of VS-NfD.

IT requirements for the processing of information classified VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

1 Introduction

1.1 General remarks

If information technology (IT) is used for the processing of information classified VS-NfD, suitable technical and organisational measures must be taken to protect VS-NfD in addition to the general protective measures set out in Parts 1 and 2 of this Code of Practice, and compliance with these measures must be regularly monitored. Suitable technical measures include IT security products carrying an approval statement (approval or authorisation for use) from the BSI and are used in the intended context of use. Unless other specifications have been made by the VS-NfD principal or the BSI, the technical and organisational measures for protecting VS-NfD on IT systems are stipulated in No. 2. Irrespective of the IT system used, the requirements for the processing of VS-NfD under No. 3 must be complied with.

1.2 Classified information from international organisations (NATO, EU, etc.)

When classified information of supranational or intergovernmental institutions and agencies with a classification level comparable to that of VS-NfD is processed, the respective regulations of these institutions/agencies apply.

2 IT system

The technical and organisational measures to protect VS-NfD on IT systems depend on the type of the IT system. There are two types:

1. An IT system that is technically isolated (air-gapped) (No. 2.1) or
2. An IT system that is connected to other networks that have a lower security level than VS-NfD (No. 2.2).

A technically isolated (air-gapped) IT system can be a stand-alone PC (No. 2.1.1) or an IT system network (No. 2.1.2). The latter can also exist cross-location. In this case, an IT security product carrying an approval statement from the BSI must be used for the transmission.

The processing of VS-NfD on a company's own IT system is permissible if the following conditions are met:

2.1 VS-NfD on a technically isolated (air-gapped) IT system

2.1.1 Stand-alone PC

The following technical and organisational security measures are to be implemented:

- Access control:
  - The IT equipment is only to be used by persons authorised to access VS-NfD and who are obligated to comply with this VS-NfD Code of Practice
  - User profiles/restrictive[1] access rights and logins/passwords are to be set up to implement the need-to-know principle

[1] Operating systems are normally configured such that each user automatically receives full access to all contents on the data carrier with the exception of the personal folders of other users. User access to individual folders must be explicitly deauthorised (opt-OUT). The principle of 'need-to-know', on the other hand, means that explicit permission must be granted where folders need to be accessed by users who are not also their creators (opt-IN).

- IT systems that do not have hard disk encryption carrying an approval statement must be switched off before the end of work and remain switched off and stored in accordance with Part 2, No. 5
- Appropriate measures must be taken in patch and change management as well as for protection against malware, and it must be ensured that no leaks of VS-NfD can take place unnoticed
- The use of wireless interfaces is not permitted
- Wire-based interfaces that have not been approved for use are to be deactivated
- There must be appropriate hard disk encryption for mobile IT systems
- Encryption/decryption of VS-NfD is to be undertaken using an IT security product carrying a BSI approval statement; any bidirectional data that is transferred between an open workstation PC and the stand-alone PC using a mobile data carrier has to be encrypted. It must be ensured that the plaintext data is not stored on the mobile data carrier – not even temporarily, for example, as part of the encryption/decryption process.

The BSI's compendium of basic IT protection (IT-Grundschutz) does not have to be applied here.

2.1.2 Connection of an IT system

In addition to the security measures listed under No. 2.1.1, the following are also to be implemented:

- Minimum data storage requirement: data from different VS-NfD contracts must be stored in separate project folders that are released for use to the respective authorised users only; the VS-NfD principal may specify further requirements, e.g. the IT system is exclusively to be used for the respective project.
- Central VS-NfD components: central VS-NfD components must be physically secured in the server room in accordance with the 'need-to-know' principle. This can be done by partitioning in the form of a cage or a comparable keying off (lockable server racks with individual locks, etc.).
- Communication relationships: all communication relationships, especially those cross-site, are to be described in an information security concept (see point 4.2) and evaluated as to whether the VS-NfD needs to be encrypted by an IT security product carrying an approval statement (see No. 3.4.1).

An information security concept that focuses on the IT system and complies with the applicable standards of the BSI's IT-Grundschutz is only required here if an interconnected IT system is used. In this case, the basic requirements must be implemented at the very least (No.4.1). The VS-NfD principal may specify further requirements.

2.2 VS-NfD network connected to network segments that do not meet VS-NfD requirements

In addition to the security measures listed in No. 2.1.2, the following must also be implemented for the VS-NfD network:

- Segment separation: physical or authorised separation of the VS-NfD network segment from other network segments, for example by means of a multi-level firewall system following the PAP structure in accordance with the BSI IT-Grundschutz

Special regulations, e.g. for project group folders where all users automatically have access to the stored data, must be documented in the information security concept.

- Firewall: a set of rules must be created for the firewall (PAP structure) and be regularly adapted and reviewed. This set of rules must also cover communication connections to outside. Access may only be initiated from the VS-NfD network. Furthermore, software updates, telemetry functions and corresponding configuration recommendations that prevent the leak of or access to VS-NfD must be implemented and regularly checked for changes, especially after each update. In the event of any abnormalities, further protective measures must be taken immediately.
- External interfaces: all interfaces must be defined in relation to communication with the VS-NfD network segment, described in the information security concept and included in the risk analysis (see No. 4.2).
- Protection against malware: the content check for malicious code must be carried out on the ALG (Application Layer Gateway) for data traffic coming from external networks. Furthermore, all IT systems must be equipped with software to detect malicious code. This software must not be used to perform malicious code checks outside the VS-NfD network, for example in the cloud.

The BSI's IT-Grundschutz has to be applied here. Basic and standard requirements (No. 4.1) must be implemented.

3 Requirements for the processing of VS-NfD

The specific requirements for the electronic processing of VS-NfD are set out below. Such processing is considered to begin as soon as VS-NfD is read on IT equipment.

3.1 Permitted IT systems and approval

IT systems to be used to process VS-NfD must be approved by the person responsible for VS-NfD before they are used for the first time. The same applies to physical work areas intended for the processing of VS-NfD.
Private IT, software and data carriers must not be used to process classified information.

3.2 Marking of data carriers and devices

Data carriers on which VS-NfD is stored unencrypted must be marked in accordance with Part 2, No. 4 of this Code of Practice. The same applies to devices in which these data carriers are located.

3.3 Maintenance and servicing

Where data carriers are storing unencrypted VS-NfD, the VS-NfD must be completely erased in accordance with No. 3.6 before the data carriers leave the personal safekeeping of the persons authorised to access it in the course of maintenance or repair work on the IT system.
If the data cannot be erased, the data carriers are to be removed and retained. If this is not possible, Part 2, No. 6.3 of this Code of Practice applies.

3.4 Transmission of VS-NfD via technical communication links

3.4.1 Encryption requirement for electronic transmission

VS-NfD must always be encrypted during electronic transmission, with the exception of No. 3.4.2. Only IT security products[2] carrying an approval statement are to be used for this purpose.

3.4.2 Requirements for unencrypted transmission within company premises

If the transmission of VS-NfD within company premises is exclusively line-based and all transmission facilities, lines, distributors and routes are protected against unauthorised access, encryption is not required.

3.4.3 Use of telephones/fax machines:

End-to-end encrypted telephony and transmission by fax are permitted after a risk assessment has been carried out. No. 1.1 applies.

3.4.4 Mobile IT systems

If portable IT systems are used for processing or storing VS-NfD, the classified information must be encrypted using IT security products carrying an approval statement. If the IT systems remain on the premises, either in personal safekeeping or under physical protection (Part 2, No. 5), encryption is not required.

3.4.5 Transmission of VS-NfD in emergency situations

By way of derogation from No. 3.4.1 ff., VS-NfD may by way of exception be transmitted via communication links not approved for VS-NfD if transmission via a BSI-approved encrypted communication link cannot be provided within a reasonable timeframe. The details of the divergent framework conditions and requirements will be determined separately for the respective emergency situation by the VS-NfD principal.
If the involvement of the VS-NfD principal would lead to a delay in which the resulting harm would significantly outweigh the harm associated with disclosure of the VS-NfD, the person responsible for VS-NfD may by way of exception approve the transmission autonomously. In this case, the VS-NfD principal must be informed immediately. Notification obligations of companies subject to confidentiality as per the GHB will remain unaffected. In each individual case, the consent of the person responsible for VS-NfD must be obtained and documented.
In the exceptions described, the following precautions must be observed in order to reduce the risk of information leaks as much as possible:

- The identity of the communication partner is to be established before the communication begins.
- The communication is to be conducted in such a way that the content of the VS-NfD cannot be understood by third parties and the fact it is classified such remains obscure.

[2] The current list of approved IT security products and systems (BSI document 7164) can be found on the BSI website at https://www.bsi.bund.de. The respective conditions of use and operation (SecOps) are available for download in the protected area of the Federal Ministry for Economic Affairs and Climate Action security forum. Companies not previously tasked with processing VS-NfD will receive these from their VS-NfD principal. The specifications described in the conditions of use and operation must be implemented. Installations and configurations that differ from this are not permitted. If there are no IT security products carrying an approval statement, the communication link must not be used.

- The transmitted VS-NfD is not to have been marked as such or contain any indications distinguishing it from unclassified information. The obligation to label VS-NfD is lifted in this case.
- The communication partners are to be informed immediately of the VS-NfD classification by other means (for example, via other technical communication links, by post or courier), unless this is not possible or not appropriate in the individual case. Where possible, the communication partner is to subsequently label the VS-NfD as such.

3.5 Taking VS-NfD away from company premises and working from home

VS-NfD in electronic form only may be processed from home under the following conditions:

- The IT used (e.g. notebooks) has been approved for this purpose by the person responsible for VS-NfD (No.3.1)
- The private residence is located within Germany
- The person responsible for VS-NfD has given consent
- The employee has been informed about the specific risks of working from home
- Part 6 of this Code of Practice has been signed by the employee and is retained by the company as proof

3.6 Erasing and destroying storage media containing VS-NfD

Before storage media permanently leave the VS-NfD workspace, they must be erased using BSI-approved or permitted IT security products. If erasing is not possible, the storage media must be physically destroyed in accordance with the applicable BSI specifications.

3.7 IT administration

IT administration must always be carried out by in-house company staff. Part 2, No. 6.3 of this Code of Practice applies.

4 BSI's compendium of basic IT protection (IT-Grundschutz)

Depending on the selected type of IT system, the most current version of the BSI's IT-Grundschutz must be applied to varying extents (No. 1.1 f.).

4.1 Security requirements

The BSI's IT-Grundschutz in its most current version is divided into various process and system-oriented modules. Each module lists the security requirements for the protection of the particular item considered and describes what needs to be done to protect it. The requirements are divided into different categories, in particular into

- Basic requirements
- Standard requirements that build on the basic requirements

The necessary amount of implementation for the respective type of IT system is based on No. 2. The requirements under No. 3 are an additional component in the application of the IT-Grundschutz.

4.2 Information security concept and risk analysis

An information security concept must be drawn up for the IT system, covering the application of the BSI's IT-Grundschutz including all the relevant security requirements. The company must set out which of the modules in the BSI's IT-Grundschutz apply to the IT system. In addition, the requirements as per the VS-NfD Code of Practice must be included, as well as a

risk analysis. In the event of changes, the information security concept, including the risk analysis, must be updated.

5 Self-accreditation

The person responsible for VS-NfD at the company is to provide written confirmation to the executive board of the company every three years at the latest that the requirements from Part 3 (IT requirements) of this Code of Practice are being implemented (self-accreditation). Upon request, this confirmation is to be passed on to the VS-NfD principal or the Federal Ministry for Economic Affairs and Climate Action.

In the self-accreditation, the company attests to the following:

1. The implementation of the IT requirements in the most current version of this Code of Practice
2. If necessary, the implementation of the conditions of use and operation of the IT security products carrying an approval statement
3. The establishment of an ISMS through:
    - The application of the applicable standards from the BSI's IT-Grundsatz incl. the creation of an information security concept featuring an IT-Grundsatz check, risk analysis and implementation planning or
    - ISO 27001 certification on the basis of the IT-Grundschutz or
    - ISO 27001 certification on another basis incl. analysis of the differences to the IT-Grundschutz (mapping table/gap analysis), if an equivalent or higher security level to the requirements of the IT-Grundschutz is ensured

Notes on the marking of information classified VS NUR FÜR DEN DIENSTGEBRAUCH

1. Information classified VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) is to be marked at the top using the classification level written out in full in black or blue. Where the VS-NfD consists of more than one page, the top of each page of writing is to be marked. The same applies to classified annexes.
   In addition, it must be stated who the creator or the originator of the VS-NfD is and when the information was created or classified.
   If the nature of the VS-NfD does not permit such marking to be undertaken, it should however be handled in an equivalent manner (e.g. marking in the associated documentation)

2. The classification period is only to be indicated if it is less than the standard period of 30 years. In this case, the classification period must be indicated on the first page of the VS-NfD using the following annotation: “The classification finishes at the end of the year … .”
   The classification of VS-NfD is declassified after 30 years at the latest and cannot be renewed. The classification period finishes at the end of the year in which the end of the period falls.

Proof of obligation to comply

Applicable parts are marked with a cross

Mr/Ms

Surname, First name Date of birth

has today been informed about the provisions of sections 93 to 99, 203(2) and 353b of the German Criminal Code (StGB), instructed about the special provisions on VS-NfD protection and obligated to fulfil them conscientiously with regard to their intended access to information classified

VS-NUR FÜR DEN DIENSTGEBRAUCH

This obligation also applies to the time after they leave their current employment relationship. They are aware that in the event of violations of the above-mentioned provisions, they may be subject to contractual or labour law measures and criminal prosecution for the violation pursuant to sections 93 to 99, 203(2) and 353b of the StGB. They have received a copy of this obligation. They have been provided with a copy of the VS-NfD Code of Practice

☐ Part 2 (General provisions)
☐ Part 3 (Provisions on the use of IT)
☐ Part 4 (Provisions on marking)
☐ Part 6 (Handling of VS-NfD in the home)

.

Original german version to be signed only

[Signature of the person under obligation]

Agreement on the handling of information classified VS-NUR FÜR DEN DIENSTGEBRAUCH in the private home (working from home)

1 Maintaining the required level of protection

When handling VS-NfD at home, the level of protection specified in the VS-NfD Code of Practice must be implemented. The employee undertakes to take the necessary measures to implement this level of protection in their private home. The private home refers to the residence of the employee in the Federal Republic of Germany.

2 'Need-to-know' principle

The 'need-to-know' principle must be observed. VS-NfD is to be protected in particular from being viewed by other persons in the private home. To ensure this protection, suitable organisational or technical measures (e.g. use of a separate room, simple lock for papers and material, compliance with Part 3 of this Code of Practice in the case of IT processing) must be taken that are appropriate to the specific risks of handling classified information in the private home.

3 Use of information technology (IT)

Where VS-NfD is stored on IT, Part 3 of the VS-NfD Code of Practice must be complied with. In particular, the employee must comply with the following measures:

- The IT-based processing of VS-NfD in the private home may only take place on IT systems (hardware and software) approved by the person responsible for VS-NfD
- IT systems that do not have hard disk encryption carrying an approval statement must be switched off before the end of work and remain switched off in accordance with Part 2, No. 5
- The IT systems used must not be connected to IT devices inside the private home or outside of it (exception: private internet routers used for a VS-NfD communication connection approved by the person responsible for VS-NfD)
- Maintenance or repair work on IT system components may only be carried out at the behest of the person responsible for the protection of VS-NfD at the company
- The IT systems may not be used for private purposes
- The instructions for use of the IT systems issued by the person responsible for VS-NfD must be complied with

The employee has been instructed about specific risks pertinent to working from home and confirms that they will implement the relevant requirements in the VS-NfD Code of Practice and this agreement.

Original german version to be signed only

[Signature of the employee Signature of the person responsible for VS-NfD]