Federal Ministry
for Economic Affairs
and Energy

I n s t r u c t i o n S h e e t

on the Handling of
Information Classified
VS - NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)
(RESTRICTED)
– in Industry –

(VS-NfD-Merkblatt)

This Instruction Sheet determines the handling of national information classified VS - NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD), of foreign information and of information of international organisations (e.g. NATO, EU, OCCAR) with an equivalent classification level - hereinafter referred to as VS-NfD - in industry. In order to protect Classified Information of international organisations (i.e. NATO, EU, OCCAR) additional rules have to be respected which may deviate from national provisions. A list of equivalent classification levels and further information on VS-NfD regulations can be obtained from the security officer or - if no security officer has been appointed - from the contracting authority. Specific questions can be directed to the Federal Ministry for Economic Affairs and Energy, BMWi, division RS 3, under the following e-mail address: DSAGermany-RS3@bmwi.bund.de.

I. General

1. Access and release

1.1 Information classified VS-NfD shall be made accessible only to persons who have a need to know in connection with the execution of a given contract or pre-contract activities or negotiations (“Need-to-Know” Principle). All persons who are granted access to information classified VS-NfD shall be informed in a verifiable way of this Instruction Sheet before having access to the relevant information. They shall be made aware of their special responsibility for the protection of such information in accordance with the provisions of this Instruction Sheet and of the consequences under criminal law and of contractual penalties in case of violations.
Further measures, such as BMWi security protection procedures, security clearances and formal visit requests are not required.

1.2 The content of the Classified Information shall not be disclosed to third parties. Employees who have proved to be unsuited for the handling of such Classified Information or who have violated the security obligations shall be excluded from work on that Classified Information.

1.3 Information classified VS-NfD may be released only to government bodies, international organisations or contractors which are involved in a programme/project/contract and which must have access to the information in connection with the execution of the programme/project/contract. The release of information classified VS-NfD to international organisations or contractors from countries which are not involved in the programme/project/contract requires the prior written approval of the contracting authority. As a basic principle, a security arrangement with the respective international organisation or the country in which the contractor is located is necessary. In case the contracting authority can not be determined any more, the approval can be obtained from BMWi.

1.4 Within Germany, BMWi can ascertain if contractors comply with the rules contained in this Instruction Sheet.

1.5 Information shall be declassified after thirty years unless no other period is stipulated. This period begins on 1. January of the year following the classification. In the case of international

contracts, BMWi must be consulted provided no Programme or Project Security Instructions (PSI's) exist.

2. Processing Guidelines

2.1 Marking and Handling/Storage

Documents and material classified VS-NfD shall be marked, handled and stored as follows:

2.1.1 Documents shall be marked using black or blue stamp imprint with the classification level "VS - NUR FÜR DEN DIENSTGEBRAUCH" at the top of each written page and of all equally classified annexes. International or foreign Classified Information shall be stamped with the equivalent German classification level. In the case of books, brochures etc., the marking on the front cover and the title page shall be sufficient. If each page of a foreign book or brochure is marked with the foreign classification level, the equivalent marking of the front cover or the title page shall be sufficient.

2.1.2 Material classified VS-NfD (e.g. equipment or components) or data storage media (e.g. floppy disks, compact disks, microchips, microfiches) shall also be marked visibly on the material itself or - if this is not possible - on the containers holding the material.

2.1.3 The "Need – to Know" Principle has to be observed at all work steps in the company. This is valid especially also for reprography, if the reprography devices use data storage media.

2.1.4 Classified Information shall be stored in locked rooms or containers (cabinets, desks etc.). Outside such rooms or containers, such material shall not be stored or handled in a manner that could result in unauthorised access or an insight into the classified information.

2.1.5 Handling of Classified Information in private locations (Telecommuting Jobs) is an exception to the rules laid out in this Information Sheet.

This is only permitted for information classified VS NfD, which has been classified after … (date at which the new "General Administrative Regulations Governing the Material and Organizational Safeguarding of Classified Information – VS – Anweisung" come into force), if a written approval from the contracting authority is at hand. The approval will be assumed, if the compliance with this Instruction Sheet has been contractually agreed upon between the contracting authority/awarding contractor and the contractor/subcontractor and the contracting authority/awarding contractor has not expressively contradicted.

In individual cases the contractor can contractually prohibit the handling via Telecommuting Jobs of information classified VS-NfD which has been classified as such before….(date at which the new "General Administrative Regulations Governing the Material and Organisational Safeguarding of Classified Information – VS – Anweisung" come into force).

The Company Security Officer (or the person assigned by the company) has to assess every individual case. The Company Security Officer has to brief the respective employee in a verifiable manner. Before the Telecommuting Job will be commenced, the Company security officer has to ascertain that the necessary requirements for the handling and storage of Classified Information according to this Information Sheet are available at the employee's premises. The employee has to allow control in his/her private premises by the Company Security Officer or BMWi.

2.1.6 Interim Classified Information (e.g. drafts, stenogrammes, sound recording media, Overlays) shall be protected from compromise by unauthorised persons in the same way as the document to

which it refers. Interim information that is not transmitted to third parties and destroyed immediately, shall not be marked as Classified Information.

2.2 Transmission

2.2.1 Within Germany, information classified VS-NfD shall be transmitted by couriers or postal services in a single closed envelope or a container. The envelope or container do not bear a classification marking.

2.2.2 Classified Information may be transmitted to foreign countries by commercial courier services as a standard letter or parcel, or as air or sea freight, unless the contracting authority has explicitly excluded this type of delivery or laid down other modalities for delivery to foreign countries. In this context, the contracting authority/awarding contractor shall take account of intergovernmental agreements and special Programme or Project Security Instructions (PSI's).

2.3 Destruction/Return

2.3.1 In order to prevent large stocks of classified items, Classified Information that is no longer needed shall either be destroyed or returned to the contracting authority.

2.3.2 Classified Information, including interim Classified Information, shall be destroyed in a manner that its content is no longer recognisable and cannot be rendered recognisable again.

2.4 Loss, unauthorised disclosure, discovery of Classified Information or failure to comply with the Instruction Sheet

The loss, unauthorised disclosure and discovery of Classified Information or non-compliance with this Instruction Sheet shall immediately be notified to the German contracting authority and the Federal Ministry of Economics and Technology (BMWi, division RS 3) via the appointed company security officer. If there is no company security officer a person which is responsible for the protection of information classified VS-NfD in the company has to be appointed. They will take the necessary steps to control possible damage and investigate the incident.

2.5 Visits

Visits to or from foreign countries which involve access to information classified VS-NfD or of equivalent classification levels shall usually be agreed upon directly between the dispatching facility and the facility to be visited. No specific formal procedures have to be observed.

2.6 Contracts

2.6.1 Contracting authorities/awarding contractors shall contractually oblige all contractors/subcontractors to comply with the rules of this Instruction Sheet. In this context, they shall point out that non-compliance may result in the termination of the contract or of parts of the contract.

2.6.2 During tenders or invitations to tender and after the execution of contracts it shall be ensured that Classified Information is stored properly until its declassification, and destroyed or returned to the originator as soon as possible.

2.6.3 Foreign contractors/subcontractors shall contractually be obliged to comply with the directives of their competent security authority on the handling of Classified Information of

equivalent classification levels. If there is no equivalent classification level in the country of a contractor/subcontractor, BMWi (division RS 3) must be contacted and will make arrangements on protection rules with the competent foreign security authority. In this case, release of the relevant information requires the prior approval of BMWi.

II. Use of Information Technology (IT)

1. Processing

1.1 If information technology is used for processing of information classified VS-NfD, appropriate IT measures and/or other physical and organisational measures shall be taken for the protection of the Classified Information (in accordance with part I sections 1.1 and 1.2).

1.2 Before information classified VS-NfD may be processed or stored it must be guaranteed that the terminal or the internal network are not directly linked to the Internet (without protection e.g. by means of a firewall) unless further measures pursuant to part II section 3.3 have been taken.

1.3 The following measures, in particular, shall be considered when processing information classified VS-NfD:

- compile lists of all persons who are authorised to have access,
- use of identification and authentication mechanisms (e.g. login, password),
- create appropriate IT security instructions (in relation to individual workplaces or companies).

The use of wireless keyboards and wireless networks requires accrediting by the Bundesamt für Sicherheit in der Informationstechnik (BSI - Federal Information Security Agency).

1.4 If portable IT systems (e.g. notebooks or handhelds) are used for the processing or storage of data classified VS-NfD, the used storage media shall be encrypted by products accredited by the BSI.

1.5 Portable data storage media (e.g. floppy disks, CD's, removable hard disks) that contain unencrypted[1] data classified VS-NfD, shall be marked in accordance with part I section 2.1.2 and stored in accordance with part I section 2.1.4.

1.6 Data storage media shall be erased by means of software products that provide for at least double overwriting. Products recommended by the BSI should be used.

1.7 Information technology and data storage media shall be checked for viruses (in particular trojan horses or worms) before they are used for processing information classified VS-NfD. These checks shall be repeated at regular intervals.

1.8 Private information technology devices (e.g. laptops), software and data storage media must not be used for processing information classified VS-NfD. Private software or private data storage media must not be used on information systems that are used for processing information classified VS-NfD.

[1] to encrypt = to encipher or to encode. In order to be able to do without physical security measures (classification marking, secure storage etc.), the system used for encryption must be licensed by the BSI and/or authorised by the BMWi.

1.9 On fixed data media containing data classified VS-NfD in an unencrypted form, the classified information shall be deleted in accordance with para 1.6 before the data media, for the purpose of maintenance and repair work on IT system components, leave the perimeter of persons authorized to have access. If deletion is not possible, the data media shall be removed and retained or the company entrusted with the maintenance/repair work shall be placed under the contractual obligation to comply with the provisions of this Instruction Sheet.

2. Transmission

2.1 In the case of electronic transmission via telecommunications or other technical communications links (including online services such as WWW, FTP, TELNET, e-mail etc.) within Germany, Classified Information shall be encrypted by means of an encryption system that is licensed by the BSI or authorised by BMI (Federal Ministry of the Interior), or, in individual cases, by BMWi.

Notwithstanding this provision, as an exception, unencrypted transmission shall be admissible in the following cases:

a) Within fixed networks for telephone conversations, video conferences and fax and telex transmission provided that encryption is not possible for the required type of transmission between the sender and the recipient and the contracting authority has not explicitly required encryption when awarding the contract. Before starting transmission, the sending facility must ensure that it is connected with the correct recipient.
b) Within a self-contained network (LAN) provided that it is used exclusively on a locally contiguous company-owned premises and that the transmission facilities are protected from immediate access by unauthorised persons.

2.2 In the case of cross-border electronic transmission, the encryption methods shall be agreed upon by the competent security authorities of the countries involved. If specific security provisions for transmission have been agreed upon for a programme/project, these must be observed.

If necessary, BMWi (division RS 3) shall provide further information.

3. Measures to guarantee the confidentiality of information classified VS-NfD when information technology (IT) is used

The following measures aim to ensure the confidentiality of electronically stored classified information. It is not their main objective to guarantee the integrity and availability of data. Three different initial situations can be identified:

3.1 Stand-alone PC or networks with self-contained user groups that are not linked to other networks

- The operating system shall allow for a differentiated user profile and access protection up to data level for individual data files in order to guarantee the “Need-to-Know” principle.
- A login and a password must be existent. The password shall comprise of at least 6 digits, alphanumeric (special characters), with lower and capital letters.
- The BIOS shall also be protected by a password.
- The booting of the IT system must be possible only from the hard disk.
- If possible, a RAM disk should be available for the temporary data files (user aid).

- An updated antivirus software must be used.
- In the case of networks, a separate partition for the storage of Classified Information should be installed on the server.

3.2. Self-contained networks with e-mail connection to users outside these networks

In addition to the provisions laid down in part II section 3.1 there must

- a server-based network be existent with the server located in an access controlled area
- a firewall be existent either on the server or as a separate IT system (or an additional mail server, if available); also located in an access controlled area.
- a packet filter be used; an applications gateway is possible as an option.
- any further IP - address other than the server IP be concealed from the outside (DNS server).
- information classified VS-NfD be transmitted in encrypted form only with products that are approved by BMWi. Encryption keys basically must not be stored on hard disks.

Mandatory user rules shall be laid down within the company and users shall be trained. The most recent security updates of the software employed shall be installed as soon as it is available and the firewall shall be adjusted accordingly.

3.3. Stand-alone PC's or self-contained networks with e-mail and Internet access

In addition to the provisions laid down in part II sections 3.1 and 3.2 these must

- provide a firewall and an application gateway.
- apply the provisions of the BSI - IT – Basic Protection – Handbook for password rules.
- keep information classified VS-NfD on the server within an either separate partition or in a specially protected data sector; the thereby given protection mechanisms shall be applied accordingly.

Depending on the scope, a separate VPN e.g. for a user group or a project is required.