

Instruction sheet on the Handling of Protectively Marked Information
Classified
VS-NUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED)
(short title: VS-NfD-Merkblatt;
Instructions on the Handling of RESTRICTED information)

This instruction sheet is intended to inform members of public agencies about the general handling of protectively marked information classified VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD – RESTRICTED), and in particular for the drafting of contracts with private companies and organisations on the provision of services classified as VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD – RESTRICTED). The provisions contained in these instructions should be taken into account when drafting such a contract.

I. General

1. Access and Disclosure

1.1. Items classified VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD – RESTRICTED) shall only be made accessible to such persons as must, in connection with the execution or negotiation of the given contract, have access to such information (“need-to-know” principle). Persons authorized to have access shall be informed of this Instruction Sheet before they get access to such classified information; the fact that they have been informed of this Instruction Sheet shall be kept on record; it shall be pointed out to them that they bear a special responsibility for the protection of the classified items pursuant to this Instruction Sheet and that any violation of the provisions contained therein may result in consequences under criminal law or the law of contracts.

Any further measures such as a security procedure of the Federal Minister of Economics and Technology, security screenings or the formal announcement of visits are not required with this classification level.

1.2 The contents of the given classified item shall be kept secret from outsiders. Staff members who have proved to be unsuited for handling such classified items or who have failed to comply with their duty to observe secrecy, shall be excluded from work on the respective classified items.

1.3 Items that are classified VS-NFD (RESTRICTED) may be disclosed only to government agencies, intergovernmental organisations or contractors which are involved in a programme/project/contract and must have access to the classified information in connection with such programme/project or contract. Prior to the disclosure of items classified VS-NFD (RESTRICTED) to intergovernmental organisations that are not involved in the programme/project/contract or to contractors from countries that are not involved in the programme/project/contract, the written consent of the contracting authority (i. e. the authority which has awarded the classified contract) shall be obtained. As a matter of principle, a security agreement shall be required in this context (cf. also section 23 of the General Administrative Regulations Governing the Material and Organisational Safeguarding of Classified Information).

1.4 In Germany, the Federal Ministry of Economics and Technology can ascertain whether the provisions of this Instruction Sheet are complied with by contractors which have been awarded a classified contract. In cases where the contract is awarded by a public authority, the latter may exercise the control rights pursuant to sentence 1.

1.5 The security grading shall expire thirty years after the first day of January of the year which follows the date of classification, unless another term has been defined. In the case of international contracts, the Federal Ministry of Economics and Technology shall be consulted if there are no programme or project-related security instructions in place (cf also section 26 of the General Administrative Regulations Governing the Material and Organisational Safeguarding of Classified Information).

Processing of classified information

2.1 Marking and Handling/Storage

Documents and material classified VS-NFD (RESTRICTED) shall be marked, handled and stored as follows:

2.1.1 Documents shall be marked with the stamped or printed security grading "VS-NUR FÜR DEN DIENSTGEBRAUCH" in blue or black at the top of each written page and of all annexes similarly classified; international or foreign classified documents shall be re-stamped with the corresponding German marking. In the case of books, brochures etc. it shall be sufficient to apply the marking to the cover and the front page. In cases where every written page of a foreign book or brochure carries the foreign security grading, it shall be sufficient to apply the German security grading to the cover or the front page.

2.1.2. Material classified VS-NfD (RESTRICTED) (e.g. equipment) or data media (e.g. discs, CDs, microchips, microfiches) shall also be clearly marked or re-stamped either on the material itself or, where this is not possible, on the storage containers of the material.

2.1.3. Classified information shall be stored in locked rooms or containers (cabinets, desks, etc.). Outside such rooms or containers it shall at all times be stored and handled in such a way that unauthorized persons do not get access to and are not able to observe the contents of classified information.

2.1.4 Interim material (e. g. preliminary drafts, shorthand notes, sound recording material, overlays) shall be afforded the same protection against observation of their contents by unauthorized persons as is given to the respective job file. Interim material that is not passed on to third parties and is immediately destroyed needs not to be marked as classified.

2.2 Transmission

2.2.1. Inside Germany, transmission shall be by couriers or by a postal service, in a closed envelope or container. The envelope or container shall not bear any security marking.

2.2.2. Classified items may be dispatched to foreign addresses by private courier companies as standard letter or parcel or by air or sea freight unless the contracting authority has expressly objected to this type of shipment or laid down other modalities governing the dispatch to foreign addresses. In this context, the contracting authority shall take into account any intergovernmental agreements and/or special programme or project-related security instructions.

2.3 Destruction/Return

2.3.1. In order to avoid extensive holdings of classified material, any classified items that are no longer required shall be destroyed or returned to the contracting authority.

2.3.2 Classified items, including interim material, shall be destroyed in such a way that the contents are no longer recognisable and cannot be rendered recognisable again.

2.4 Loss, unauthorized disclosure, discovery of classified items or failure to comply with this Instruction Sheet

Any loss, unauthorized disclosure and discovery of classified items and any failure to comply with this Instruction Sheet shall be immediately reported through the security officer of the public authority or the private organisation concerned – if it has appointed such a security officer – to the German contracting authority and to the Federal Ministry of Economics and Technology (unit VI B 3), in order to contain any potential damage and to investigate the incident.

2.5 Visits

Visits abroad or from abroad which involve access to material classified VS-NfD (RESTRICTED) or material similarly classified shall as a rule be agreed between the sending institution and the institution that is to be visited. There are no specific formal regulations.

2.6 Contracts

2.6.1. The contracting authority shall place all contractors and sub-contractors which have been awarded a classified contract, under the contractual obligation to comply with the regulations of this Instruction Sheet. In this context, it shall be pointed out that any failure to comply with this Instruction Sheet may result in the cancellation of the contract or of parts thereof.

2.6.2. In the case of proposals or calls for proposals and following contract execution classified items shall be stored as prescribed, destroyed or returned as soon as possible, unless and until they are downgraded.

2.6.3. Foreign contractors and sub-contractors shall be bound by contract to comply with the regulations issued by their competent security agency on the handling of items similarly classified. In cases where there is no comparable security grading in the country of a contractor/sub-contractor, the Federal Ministry of Economics and Technology (unit VI B 3) shall be involved; the latter shall then proceed to agree with the competent foreign security authority on the necessary security regulations. In such cases, the classified items may be disclosed only once the Federal Ministry of Economics and Technology has given its consent.

II. Use of Information Technology (IT)

1. Processing

1.1 If information technology is used for processing items classified VS-NfD (RESTRICTED), appropriate IT measures and/or physical and organizational measures shall be taken in order to ensure the protection of the classified information (cf. part I paras 1.1 and 1.2).

1.2. Prior to the processing or storage of items classified VS-NfD (RESTRICTED), it shall be ensured that the computer or the internal network are not directly linked to the Internet (e.g. without firewall protection), if no further measures pursuant to para. 3.3. have been taken.

1.3. The following measures, in particular, shall be considered when processing items classified VS-NfD (RESTRICTED):

- listing of the persons authorized to have access;
- use of identification and authentication mechanisms (e.g. log-in, password);
- an appropriate IT Security Instruction (for the individual workplace or for the company as a whole).

Radio keyboards and radio networks may be used only if they are accredited by the Bundesamt für Sicherheit in der Informationstechnik (BSI – Federal Office for Information Security).

1.4 In cases where portable IT systems (such as notebooks or handhelds) are used for the processing or storage of data classified VS-NfD (RESTRICTED), the storage media used shall be encrypted by means of BSI-accredited products. Where BSI-accredited programmes and equipment are not available, it shall be permissible to use products that have been certified by the BSI according to the Common Criteria, minimum Assurance Level EAL 3.

1.5 Portable data media (e.g. discs, CDs, removable discs) containing data classified VS-NfD (RESTRICTED) in an unencrypted form shall be marked as laid down in part I para. 2.1.2. and be stored in accordance with part I para. 2.1.3.

1.6 The erasure of portable data media shall be effected by means of software products that provide at least for a twofold overwrite. For this purpose, BSI-recommended products should be used.

1.7 IT equipment and data media shall be checked for viruses (in particular Trojan Horses or worms) before they are used for processing information classified VS-NfD (RESTRICTED). This check shall be repeated at regular intervals.

1.8 Private IT equipment (e.g. laptops), software or data media must not be used for processing information classified VS-NfD (RESTRICTED). Private software or private data media must not be used on Information systems that are used for processing information classified VS-NfD (RESTRICTED).

1.9 On fixed data media containing data classified VS-NfD (RESTRICTED) 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 or 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 For the electronic transmission over telecommunications or other technical communication lines (including online services such as WWW, FTP, TELNET, E-mail etc.) inside Germany the classified information shall be encrypted by means of a cryptological system that is accredited and certified by the BSI (section 40 of the General Administrative Regulations Governing the Material and Organisational Safeguarding of Classified Information) or released by the Federal Ministry of Economics and Technology. In derogation of these provisions, unencrypted transmission is admissible on an exceptional basis in cases where:

- a) telephone conversations, video conferences, telecopies and telexes are to be transmitted via fixed networks and there are no encryption facilities available for the required transmission mode between the sender and the addressee and where the contracting authority has not explicitly stated an encryption requirement at the time when the contract was awarded. Before the transmission, the transmitting party shall, if possible, ascertain that it is connected to the desired addressee;
- b) transmission is confined to an Intranet (LAN) that is only operated on an integrated, company-owned campus and whose transmission facilities are protected against direct unauthorized access.

2.2 In the case of international electronic transmissions the encryption procedures shall be agreed between the national security agencies of the states involved. To the extent that specific security instructions concerning transmission have been agreed in the context of a programme/project, they shall be complied with. If required, the Federal Ministry of Economics and Technology (unit VI B 3) shall provide additional information.

3. Measures to ensure protection of confidentiality

The measures recommended here serve to ensure the confidentiality of electronically stored classified information. They are not primarily aimed at guaranteeing the integrity and availability of the data.

One needs to distinguish three different scenarios:

3.1 Stand-alone-PCs or networks with closed user groups that are not linked to other networks

- The operating system must ensure a differentiated user profile and access protection down to the file level in order to make sure that the "need-to-know"-principle is complied with (e. g. Unix/Linux, Win NT, Win 2000, Win XP)
- There must be a login and a password. The password must contain at least 6 alphanumeric spaces, special characters; majuscules and minuscules.

- The BIOS must also be protected by a password.
- As a matter of principle, booting of the IT system shall be possible only from the fixed disc.
- If possible, it should contain a RAM disc for the Temp files (which would make it easier and more convenient for the user to reliably delete files)
- An updated anti-virus programme must be installed
- In the case of networks, a separate partition for the storage of classified data should be installed on the server.

3.2 Intranets with external e-mail-link

In addition to the measures defined under item 3.1,

- there needs to be a server-based network, with the server located in a controlled-access area;
- there must be a firewall either on the server or in the form of a separate IT-system (and if necessary an additional e-mail-server), also in a controlled-access area; a packet filter needs to be employed; an application gateway is possible;
- any other IP-address apart from the server-IP must be concealed to the outside world (DNS-server);
- data classified VS-NfD (RESTRICTED) shall be transmitted in an encrypted form; only products released by the Federal Ministry of Economics and Technology may be used for encrypting such data; the encryption keys shall not be stored on the fixed disc. Within the company, there is a need to lay down binding user instructions and to train the staff accordingly. The most recent security updates of the software employed shall be installed as soon as they are available and the firewall shall be adjusted accordingly.

3.3 Standalone PCs or Intranets with e-mail- and Internet-link

In addition to the measures defined under item 3.1. and 3.2,

- there must be a firewall and an application gateway;
- the regulations contained in the BSI Baseline Protection Manual for Passwords; must be applied
- data classified VS-NfD (RESTRICTED) must be kept in a separate partition on the server or in a specially protected data area; the relevant protection mechanisms are to be applied accordingly.

Depending on the number of PCs involved, it will be necessary to set up a separate VPN for a specific user group or project.