General Administrative Instructions
for the physical and organisational protection of classified material
(Classified Material Instructions)
issued by the Federal Ministry of the Interior
on 31 March 2006

Contents

Enacting clause

I. General provisions
1. Scope
2. Definition of classified material
3. Classification levels
4. General principles
5. Responsibility and authority
6. Security documentation
7. Assistance from the Federal Office for Information Security

II. Management of classified material and organisational measures
8. Assignment of classification levels
9. Reclassification and declassification
10. Access to classified material and work involving the possibility of such access
11. Clearance and approval
12. Changes in clearance or approval
13. General duty to protect classified material
14. Production of classified material
15. Reproduction of classified material
16. Marking of classified material
17. Storage of classified material
18. Recording of material classified as CONFIDENTIAL or above
19. Management of material classified as RESTRICTED
20. Classified material managers
21. Principles for circulation and shipment of classified material
22. Receipt of classified material
23. Exchange of classified material with foreign countries
24. Removal of classified material from the building
25. Discussion of classified material at conferences, meetings, talks, etc.

III. Discarding of classified material
26. Principles for the discarding of classified material
27. Archiving of classified material
28. Destruction of classified material

IV. Physical and technical measures
29. Area security measures
30. Technical security of classified material
31. Guarding and technical surveillance of classified material
32. Anti-bugging measures
33. Safekeeping of keys and other means of access to classified material
34. Combination numbers as a means of access to classified material
35. Planning, procurement and acceptance testing

V. Information technology measures
36. Authorisation and operation of information technology systems
37. Products with information technology security functions for use with classified material
38. Emanations security
39. Technical testing
40. Transmission of classified material via telecommunications or other technical communications systems
41. Servicing and repair of information technology for material classified as CONFIDENTIAL or above

VI. Concluding provisions
42. Inspections
43. Reporting of any breach of security to security officers
44. Response to any breach of security or discovery of a security vulnerability
45. Special departments
46. Final provisions
47. Entry into force

List of annexes

Definitions

Enacting clause
In accordance with section 35(1) of the Federal Security Clearance Requirements and Procedure Act (Security Clearance Act) of 20 April 1994 (BGBl. I, p. 867), as amended, the Federal Ministry of the Interior hereby issues the following General Administrative Instructions for the physical and organisational protection of classified material.

I. General provisions

1. Scope

1. These Classified Material Instructions are addressed to federal authorities and public-law institutions under direct federal control which work with classified material and thus have to take precautions for its protection.

2. These Classified Material Instructions are also addressed to individuals given access to classified material or engaged in work enabling them to gain such access and required to apply certain protective measures in that connection.

2. Definition of classified material

1. Under section 4(1) of the Security Clearance Act of 20 April 1994 (BGBl. I, p. 867)*, as amended, "classified material" (CM) means any facts, objects or information needing to be kept secret in the public interest, irrespective of their form (e.g. documents, drawings, maps, photocopies, photographic material, electronic files and data carriers, electrical signals, appliances, technical equipment or spoken words). According to their need for protection, they are to be assigned classification levels by or at the instigation of an official body.

---

2. Any intermediate material arising in connection with classified material (e.g. computer files, earlier drafts, shorthand notes, sound recordings, transparencies or misprinted versions) is also to be regarded as classified material for the purposes of paragraph 1. In dealing with intermediate classified material, exceptions may be made as regards marking, recording and destruction.

3. Should the nature of classified material make it impossible to implement any of the Classified Material Instructions, they are to be applied mutatis mutandis, as far as possible taking equivalent security measures.

### 3. Classification levels

Under section 4(2) of the Security Clearance Act, according to the protection required, classified material is to be assigned one of the following classification levels:

1) TOP SECRET if unauthorised access may jeopardise the existence or vital interests of the Federal Republic of Germany or any of its Länder;

2) SECRET if unauthorised access may jeopardise the security or seriously harm the interests of the Federal Republic of Germany or any of its Länder;

3) CONFIDENTIAL if unauthorised access may harm the interests of the Federal Republic of Germany or any of its Länder;

4) RESTRICTED if unauthorised access may be to the detriment of the interests of the Federal Republic of Germany or any of its Länder.

### 4. General principles

1. Classified material may be consulted only by individuals needing to do so in the course of their duties. No-one may be acquainted with any part of classified material unless and until those duties so require. The "need-to-know" principle is to be observed.

2. Anyone entrusted with or given access to classified material, regardless of how that material came to their knowledge or into their possession, is personally responsible for the safekeeping and proper management of it and for maintaining the security of its contents in accordance with the Classified Material Instructions.

3. State-of-the-art measures are to be taken to protect classified material against any risk of a loss of confidentiality, availability* or integrity. Those measures are to be documented in accordance with Annex 5.

### 5. Responsibility and authority

1. Within their own sphere, departmental heads are responsible for the proper conduct of work involving classified material (consultation, production, reproduction, management, electronic transmission, destruction or other use) and for the implementation of the Classified Material Instructions.

2. Heads of major departments may delegate their tasks under the Classified Material Instructions, in whole or in part, to a member of their department's staff.

3. If they work with material classified as CONFIDENTIAL or above, supreme federal authorities, major higher or medium-level federal authorities and equivalent public-law institutions under direct federal control must appoint a security officer and an authorised deputy. Other authorities dealing with classified material may appoint

---

* Numbered footnotes indicate terms defined at the end.
security officers. Failing that, security officers' duties are to be performed by departmental heads.

4. Security officers must ensure that the Classified Material Instructions are implemented in their departments and advise their departmental heads on all security issues.

5. Security officers may report directly to departmental heads.

6. Departments which use information technology to process classified material are to assign information technology specialists, such as those in charge of information security, responsibility for assisting security officers in implementing the Classified Material Instructions. The information technology specialists responsible should not also act as system administrators for information technology systems used with classified material and must be given special training in the Classified Material Instructions. They may also report directly to departmental heads. Should no information technology specialists responsible for security measures be designated, their tasks will continue to be performed by security officers or departmental heads.

6. Security documentation

1. Any department working with classified material other than on an occasional basis must ensure that security documentation is kept, showing all significant plans, rules and departmental measures for maintaining security, in accordance with Annex 5.

2. Security documentation is to be updated when there are any relevant changes and should be reviewed in the event of security incidents and at least every two years as to its up-to-dateness, its completeness and the need for existing and any further security measures.

3. Documentation may be kept in electronic form. Where work on classified material needs to be individually attributable, suitable technical measures are to be taken in accordance with section 18(2). They must allow for reliable attribution to individuals and may in particular involve advanced or qualified electronic signatures.

7. Assistance from the Federal Office for Information Security

1. The Federal Office for Information Security (BSI) is to assist in implementing the Classified Material Instructions. It is to advise departments working with classified material and may, in agreement with the relevant supreme federal authority, obtain information on the operation of the Classified Material Instructions. Assistance is also to include technical testing and training. The BSI may call on the services of other bodies for support in this work; if any private bodies are to be involved, this will require prior approval by the Federal Ministry of the Interior in each specific case. Within the sphere of the Ministry of Defence, these tasks are to be performed by the Military Counter-Intelligence Office, in liaison with the BSI.

2. For the purposes of implementing these instructions, the BSI is to issue guidance on safeguarding against security threats and on ways of taking measures to protect classified material. Such guidance will need to be approved by the Federal Ministry of the Interior.

3. The Federal Office for the Protection of the Constitution, the Military Counter-Intelligence Office and the Federal Intelligence Service are to supply the BSI, without delay, with any intelligence received which may be of relevance to physical protection of classified material. Where such intelligence relates to security in trade and industry, the Federal Ministry of Economic Affairs and Technology is to be informed without delay.

II. Management of classified material and organisational measures

8. Assignment of classification levels

1. The body issuing classified material is to decide on the need for and level of classification. Material is to be classified only where necessary. Section 9(1) and (2) and the classification guidance in Annex 1 are to be applied.
2. In order to facilitate work and standardise practice, departmental heads may establish classification guidelines for commonly arising cases.

9. Reclassification and declassification

1. The issuing body or its legal successor must reclassify or declassify material as soon as the reasons for its previous classification level change or cease to apply. The issuing body or its legal successor must give notice of the change to all recipients of the classified material, in writing or by e-mail using a qualified electronic signature or some similarly secure means. Material classified as RESTRICTED may not be reclassified higher, unless notification of all recipients of the original classified material has been ensured.

2. Should the need for classification of material cease, or no longer apply to the same extent, as from a particular date or occurrence, this is to be clearly shown on the classified material or in the accompanying documentation.

3. Classified material is to be declassified after 30 years, unless any shorter or longer period is specified on it. That period runs from 1 January in the year following classification and is unaffected by any change in classification level. Specification of a longer period is subject to the following:

1) The period may be extended by up to 30 years. It may be extended only where necessary. Reasons for the extension are to be given in writing on the classified material or an accompanying note.

2) The period may be extended for individual items of classified material or en bloc for classified material arising within a particular area. Extension requires the consent of the relevant supreme federal authority.

3) The extended period is to be shown on the first page of the final draft of the classified material and on all primary copies, as follows: "Classification expires at the end of ... (year)". For classified material in other forms (e.g. appliances), this should be applied mutatis mutandis, e.g. by marking the accompanying documentation accordingly.

4) Extension of the period at a later date is to be treated as a change in accordance with paragraph 1. Should the classified material be held in the secret section of the Federal Archives, notice is also to be given to the Federal Archives.

4. For classified material over 30 years old at the time of entry into force of the Classified Material Instructions, the issuing body or its legal successor may decide to extend the classification period, in accordance with paragraph 3(1) to (4). In order for extensions to be considered, the relevant supreme federal authority may establish a blanket transition period of up to five years, for which such material initially remains classified.

5. Paragraph 3 does not apply to material classified by foreign or international bodies. Such material may be reclassified or declassified only by the issuing body, save as otherwise provided in international agreements.

10. Access to classified material and work involving the possibility of such access

1. Material classified as CONFIDENTIAL or above may not be made available to others without the consent of the relevant organisational unit (e.g. the section or division).

2. Only individuals with the appropriate clearance may work in areas in which material classified as CONFIDENTIAL or above is handled (e.g. the classified material registry).

3. Before anyone is given access to material classified as CONFIDENTIAL or above, that person must be screened and cleared for access to classified material, in accordance with the Security Clearance Act and the general administrative instructions for security clearance. Access to such classified material is to be available to individuals working on it or otherwise acquainted with its contents.
4. Before anyone is assigned work enabling them to gain access to material classified as CONFIDENTIAL or above, that person must be screened and approved for such work, in accordance with the Security Clearance Act and the general administrative instructions for security clearance. Access to classified material may be gained by individuals who:

1) transport classified material as a messenger or courier;
2) guard classified material safekeeping facilities or security areas;
3) work in a security area;
4) install, service or repair alarm systems protecting classified material;
5) manage keys or combination numbers for classified material safekeeping facilities, classified material key safes or alarm systems protecting classified material;
6) in their work on technical systems or components used in processing material classified as CONFIDENTIAL or above, can render basic security measures ineffective or gain unauthorised access to such classified material.

5. The need for clearance or approval for military security purposes is to be determined by the Federal Ministry of Defence.

11. Clearance and approval

1. Clearance and approval and any extension, restriction or withdrawal thereof are to be dealt with by departmental heads or on their behalf by security officers or specially designated members of staff. Clearance and approval are to be confined to what is necessary. They are to expire when the person concerned leaves the department, if not before. The classified material registry is to be given notice, as necessary, of clearance and approval and of any extension, restriction, withdrawal or expiry thereof.

2. Those granted clearance, or approval for work under section 10(4), are to be informed about the main security regulations, approach and recruitment methods used by foreign intelligence services and other threats and about the possibility of criminal prosecution, disciplinary penalties or employment action in the event of any breach of secrecy rules. That information is to be repeated at least every five years. Those granted clearance must be supplied with or otherwise given access to the classified material protection rules needed for their work and be required to acknowledge receipt of them.

3. The measures referred to in paragraphs 1 and 2 are to be documented (e.g. using the form in Annex 3 or electronically). Where they concern a departmental head in person, they are to be carried out by the department's higher authority.

12. Changes in clearance or approval

1. Individuals whose clearance is withdrawn or expires are required to hand in, of their own accord, any classified material held and any personal notes or records such as to require similar treatment, and to sign a statement to that effect (Annex 3, form 4). The same applies mutatis mutandis where clearance is restricted.

2. Where clearance or approval is restricted or withdrawn or expires, the person concerned is to be reminded that the duty of secrecy continues to apply.

3. The requirement not to disclose any official secrets on ceasing to be employed applies especially to information gleaned from classified material.

13. General duty to protect classified material

1. Classified material must not be discussed in the presence of anyone unauthorised or in public, particularly in transport, bars, restaurants or canteens.
2. No-one may be enticed into disclosing classified material to others by the fact that they show themselves to be acquainted with the matter in question.

3. Individuals granted clearance for access to classified material or engaged in work enabling them to gain such access (section 10(4)) should not normally be allowed to use private image or sound recording equipment, private information technology or mobile telecommunications terminal equipment (such as mobile phones, data carriers or PDAs) at work. Security officers, or organisers in charge at conferences, meetings or discussions, may introduce special rules allowing such items to be used or banning their presence altogether.

14. Production of classified material

1. Work on producing material classified as CONFIDENTIAL or above may be carried out only in units designated for that purpose. The number of copies produced and any intermediate classified material arising are to be shown on the final draft or job slip, signed by those involved, or in a record made using a qualified electronic signature or some similarly secure means.

2. For material classified as TOP SECRET or SECRET, each primary copy is to bear a serial number, placed at the top of the first page in the case of documents. For other forms of classified material, the same should apply mutatis mutandis. The document is also to show which copy is received by each individual recipient.

3. After being worked on, material in electronic form classified as CONFIDENTIAL or above is to be encrypted, using a programme approved by the BSI for the classification level, or stored in accordance with section 17.

15. Reproduction of classified material

1. Section 14 is applicable mutatis mutandis to reproductions (photocopies, printed copies, transcripts, extracts, replicas, etc.).

2. For material classified as TOP SECRET, reproductions require the issuing body's consent, which is to be shown on the classified material. For material classified as SECRET or CONFIDENTIAL, the recipient is to decide whether reproduction is permissible, after considering the need for it and while observing the "need-to-know" principle, save as otherwise stipulated by the issuing body on the classified material.

3. The number of reproductions of material classified as CONFIDENTIAL or above and the recipients of them are to be specified on the classified material to be reproduced or on a job slip. The reproductions are to be registered without delay and, for material classified as TOP SECRET or SECRET, given a serial number.

4. Reproductions of material classified as CONFIDENTIAL or above which arise from electronic transmission are to be registered without delay at the recipient's end.

5. Departments in which material classified as CONFIDENTIAL or above is commonly produced or reproduced should designate specific units with security-cleared staff for the purpose. Failing that, such classified material is to be reproduced by the classified material registry. The work is to be carried out in the presence of another individual with appropriate clearance (dual control).

6. In using photocopiers and multipurpose equipment with a non-volatile memory, section 26(4) and BSI guidance are to be applied.

16. Marking of classified material

1. The classification level is to be clearly shown in full, in capital letters, on classified material, in such a way as to be quite distinct from any other writing. Where a container or data carrier holds more than one item of classified
material, it is to be marked with the highest classification level. More detailed instructions are given in Annex 2 to the Classified Material Instructions.

2. When classified material is displayed on screen, the classification level should on each page stand out quite distinctly from the contents (e.g. by means of larger lettering and bold type). Paragraph 1 applies mutatis mutandis.

3. Where classified material is reclassified or declassified, its marking is to be amended or deleted by the relevant classified material managers or registries of the issuing department and the recipient. The amendment or deletion is to show the initials of the person who took the action and the date on which it was taken and be recorded in the classified material register. For portable data carriers and bound written material, the amendment or deletion should be shown on the item, the cover or the title page.

4. Where the nature of classified material is such that it cannot be marked in accordance with paragraphs 1 to 3 (e.g. miniaturised components), those provisions should be applied mutatis mutandis or the marking be shown on the accompanying documentation.

5. Intermediate classified material which is not passed on to others and is destroyed straight away need not be marked as classified material and recorded.

6. If not destroyed straight away, intermediate material for material classified as CONFIDENTIAL or above is to be marked with the appropriate classification level, plus the words "intermediate material". If it is passed on to others, a record needs to be kept; this does not apply if it is passed on to the classified material registry.

7. Marking of foreign or international classification levels is dealt with in Annex 4.

17. Storage of classified material

1. Material classified as CONFIDENTIAL or above is to be kept in classified material registries. It may be kept outside such a registry only where required for official business purposes.

2. While not in use, material classified as CONFIDENTIAL or above is to be locked away in classified material safekeeping facilities. For material classified as TOP SECRET or SECRET, this applies even during any brief absences of those working on it or managing it. Material classified as CONFIDENTIAL may be left in the office for any brief absences of those working on it or managing it, during working hours, provided the office door is locked using a security lock.

3. "Classified material safekeeping facilities" means steel cabinets, security vaults, etc., meeting special security requirements. More detailed instructions on classified material safekeeping facilities and guarding or technical surveillance of them are laid down in sections 30 et seq.

4. Outside working hours, such classified material safekeeping facilities are to be guarded or kept under technical surveillance by means of an alarm system. For material classified as SECRET or CONFIDENTIAL, guarding or technical surveillance of the classified material safekeeping facility may be dispensed with if the building or section of the building in which the facility is located is kept under constant guard or technical surveillance and the classified material is only temporarily stored in that facility.

5. Where classified material cannot be stored in accordance with paragraphs 2 and 3, it is to be housed in another department, which does meet the requirements. Except for material classified as TOP SECRET, classified material may be stored in a safe-deposit box if it is ensured that only authorised individuals from the department can have access to it.

6. For material classified as SECRET or CONFIDENTIAL, at the departmental head's request and after consulting the BSI, the relevant supreme federal authority may allow exceptions to the required guarding or technical surveillance, if the measures entailed would be unreasonable. For material classified as SECRET, however, it must in that event at least be ensured that any unauthorised access to the classified material safekeeping facility is immediately apparent.
7. A classified material safekeeping facility may be used by more than one individual. Where the “need-to-know” principle so requires, classified material safekeeping facilities are to be subdivided, e.g. by fitting steel cabinets with lockable inner compartments.

8. A classified material safekeeping facility whose user cannot be contacted in time is, if need be, to be opened by the security officer or a designated security-cleared individual in the presence of witnesses. Any removal of classified material is to be documented.

18. Recording of material classified as CONFIDENTIAL or above

1. Material classified as CONFIDENTIAL or above is to be managed in classified material registries. Consultation and holding of it are to be recorded by means of classified material registers, receipt books, accompanying notes, receipt forms, transfer records and destruction records (e.g. using the forms in Annex 3).

2. Such records may also be kept in electronic form, in accordance with section 6(3), as far as possible using BSI-approved classified material registration systems. In order to preserve evidence, at least the following details are to be automatically recorded in alteration-proof form:

   1) access to classified data;
   2) denials of access;
   3) on-line transmission of classified data.

Access to and especially deletion of records requires security officers' consent.

3. Classified material data carriers and their whereabouts and destruction are to be recorded in a separate classified material register. This need only show an ordinal identifier (e.g. a serial number), the area of use (organisational unit or information technology user) and a brief indication of the subject area. Classified material data carriers should not normally be passed on without obtaining a receipt. A number of items of material classified as CONFIDENTIAL or above which are held on a data carrier and not passed on do not need to be individually recorded.

4. Print-outs are to be forwarded to the classified material registry straight away and entered in the classified material register. This does not apply to intermediate classified material not passed on to others.

5. Classified material records are to be kept for at least five years. For classified material registers, this period runs from the time of downgrading to RESTRICTED, declassification, handing in or destruction of all classified material recorded in them. For classified material receipt books, receipt forms, transfer records and destruction records, the period runs from the time of issue or last entry.

6. Classified material back-up copies on data carriers are to be treated in the same way as the original classified material under these instructions, with encryption keys being held separately.

19. Management of material classified as RESTRICTED

1. Material classified as RESTRICTED and unclassified documents or items may, unless forming part of higher-classified material, be managed and stored separately from it.

2. While not in use, material classified as RESTRICTED is to be kept in locked rooms or containers (such as cupboards or desks). The need for this may be waived within security areas.

3. Further instructions for work involving material classified as RESTRICTED are laid down in Annex 7.
20. Classified material managers

1. Managers of material classified as CONFIDENTIAL or above (classified material managers) must take particular care to comply with the classified material rules and must notify security officers in the event of any breach or suspicious circumstances.

2. Classified material managers must check each day whether all material classified as CONFIDENTIAL or above which was handed out has been returned. Where material is not returned daily, they must at least every six months call for the return of all classified material which has been out for more than three months or otherwise satisfy themselves that the material is still held. Should the whereabouts of classified material not be established after two requests, they must report this to security officers.

3. Where classified material managers move from one area of work to another, their successors must check that all keys to classified material safekeeping facilities and alarm systems and all registration aids are present and satisfy themselves by means of spot checks that classified material is properly accounted for and held. Combination numbers and other access details are to be changed. A classified material transfer record is to be drawn up in accordance with Annex 3.

4. The procedure in the first sentence of paragraph 3 is to be followed where classified material managers are temporarily replaced (e.g. while on holiday or sick leave). It will suffice for the transfer to be documented.

5. Should classified material managers be unable to carry out the transfer, security officers or individuals designated by them must obtain keys and combination numbers for classified material safekeeping facilities and alarm systems and hand them to the replacements or successors, along with the registration aids. Their completeness is to be checked in the presence of a witness; the same applies to spot checking of whether classified material is held.

21. Principles for circulation and shipment of classified material

1. Before anyone circulates or dispatches classified material or its contents, they must ascertain that the intended recipient is authorised to receive or consult it. Its circulation is to be recorded and, for material classified as CONFIDENTIAL or above, it should normally, even where transmitted via telecommunications systems, be routed through the classified material registry (Annex 3, form 8).

2. In dispatching classified material, instead of sending it by mail, use should be made, where possible, of transmission via telecommunications systems, in accordance with section 40. Users of such systems must check that directories are up to date, before sending material, and must make and file a written or electronic record of the transmission.

3. Classified material encrypted using an encryption system approved by the BSI for the relevant classification level does not require any further protection against unauthorised consultation. This does not apply to cryptographic keys needed to decrypt encrypted classified material. These are to be classified and protected separately.

4. The circulation of classified material to firms is subject to the following:

   1) Security in trade and industry is to be dealt with by the Federal Ministry of Economic Affairs and Technology.

   2) Security guidance concerning the firms involved should be sought from that Ministry, before supplying material classified as CONFIDENTIAL or above.

   3) Where warranted in exceptional cases, that Ministry may also, before a contract is awarded, be asked for a definite ruling explicitly confirming that the firms involved fulfil the requirements for that particular contract.

   4) For material classified as RESTRICTED, Annex 7 is to be applied.

Where necessary for special reasons, it may also be agreed with the Federal Ministry of Economic Affairs and Technology that in certain fields the above tasks are to be taken on by another supreme federal authority.
5. Outer-office supervisors should normally take receipt of material classified as CONFIDENTIAL or above in person. With the consent of the relevant supreme federal authority, security officers may allow exceptions, e.g. so that, where there is a large amount of classified material, other outer-office staff can take receipt of it provided the outer-office supervisor is present and provided they keep it in their personal custody or in accordance with section 17(2) until it is handed over. Any such exception is to be shown in the security documentation.

6. The guidance in Annex 6 for circulation and shipment of classified material is to be followed.

## 22. Receipt of classified material

1. Consignments of material classified as CONFIDENTIAL or above received electronically or by mail are to be forwarded to the classified material registry straight away. Each consignment is to be inspected to see whether it is intact and complete. If there are any signs of unauthorised access or the consignment is incomplete, security officers and senders are to be notified without delay.

2. Classified material managers must note the date of receipt on the classified material receipt form for incoming non-electronic consignments and return the signed and stamped form to the sender without delay. For outgoing consignments, classified material managers must keep track of the return of such receipt forms.

3. Where classified material is transmitted electronically, an electronic acknowledgement of receipt will suffice. If a number of items of classified material are transmitted or received on data carriers, they are to be shown separately (e.g. in a list of file names or as a fax transmission report).

## 23. Exchange of classified material with foreign countries

1. The supply of German classified material to departments in foreign countries or in international organisations requires a security agreement/convention regulating such exchange (see Annex 4 to the Classified Material Instructions).

2. German material classified as RESTRICTED may also be supplied to foreign countries' departments without any security agreement, provided:

   1) this is necessary for official business;
   2) the recipient has been informed of the security requirement, and
   3) the foreign department gives the German department an assurance in writing that it will protect the classified material in accordance with its own national rules.

Where classified material is not infrequently supplied to another country's departments, the Federal Ministry of the Interior is to be informed with a view to concluding a security agreement.

3. In exceptional cases, material classified as CONFIDENTIAL or above may be supplied to departments in foreign countries with which there is no security agreement, provided:

   1) the requirements in paragraph 2(1) to (3) are fulfilled;
   2) the recipient states in writing that only security-cleared staff will be given access to the classified material;
   3) the German department keeps a record of the information exchanged under this paragraph, and
   4) the German department sends the Federal Ministry of the Interior a copy of the written assurance.

4. The supply of material classified as SECRET or TOP SECRET to departments in foreign countries needs to be approved by the relevant supreme federal authority in each specific case.

5. Where any delay would be prejudicial, the requirements in paragraphs 2(3), 3(4) and 4 may be fulfilled ex post facto.
6. Where classified material is received from foreign countries with which Germany has not concluded any security agreement, German departments may give the foreign department assurances in accordance with paragraphs 2(3) and 3(2) (Annex 3, forms 8d and 8e). These are to be kept for at least as long as the classified material to which they relate.

24. Removal of classified material from the building

1. Material classified as CONFIDENTIAL or above may be removed from the building or enclosed complex only in order to be taken on official trips and to conferences, meetings, talks, etc. It may not be removed for any other reason (e.g. to be worked on at home). Security officers may allow exceptions in special cases.

2. Classified material is to be taken out of the building or enclosed complex on official trips or to conferences, meetings, talks, etc., only where necessary. The rules in section 3 of Annex 6 apply mutatis mutandis. For TOP SECRET or SECRET material and on official trips aboard even for CONFIDENTIAL material, such removal requires the approval of departmental heads or, for the authorities referred to in the first sentence of section 5(3), of division or section heads.

3. Within the country, material classified as CONFIDENTIAL or above should, where possible, be sent ahead to a department at the destination which itself manages or keeps classified material. Classified material stored on data carriers in encrypted form and encryption keys for it should, as far as possible, be transported separately. Personal carriage is also permitted, provided the classified material is held on a BSI-approved information technology system or a similarly protected classified material data carriers.

4. Outside the country, material classified as CONFIDENTIAL or above should, as far as possible, be sent ahead to the relevant mission abroad and then returned by it upon completion of the official business. Where that is not possible, the Ministry of Foreign Affairs or the relevant mission abroad must package and seal the classified material and issue a certificate authorising the holder to carry the sealed item as a courier. The classified material is to be kept in the individual's personal custody at all times, or deposited at the mission abroad. Personal carriage without the assistance of the Ministry of Foreign Affairs is permitted if the classified material is held on a BSI-approved information technology system or a similarly protected classified material data carrier. Personal carriage of material classified as TOP SECRET in international transport is not permissible. Security officers may allow exceptions.

5. Material classified as RESTRICTED may be carried in a closed envelope not bearing a seal, without any courier identification.

6. It is not as a rule permissible to leave classified material unattended in hotel rooms or in hotel safes, left-luggage lockers or unoccupied vehicles.

25. Discussion of classified material at conferences, meetings, talks, etc.

1. Where material classified as CONFIDENTIAL or above is to be discussed at conferences, meetings, talks, etc., the invitation must point this out and specify the classification level.

2. Departments sending participants must ensure that only adequately cleared individuals attend and, for material classified as CONFIDENTIAL or above, must issue a conference certificate to that effect (e.g. using form 9 in Annex 3) if the host body considers this necessary for any particular reason.

3. Before the opening of the conference, meeting, talks, etc., the organisers or other side must point to the need for security in discussions and satisfy themselves that all participants have adequate clearance. Permission is required in order to take notes and any taken are to be treated as classified material. The event organiser should state in advance whether the presence of image and sound recording equipment, mobile telecommunication terminal equipment (such as mobile phones or PDAs) and other information technology is allowed or prohibited.

4. Where available, bugging-proof rooms or rooms with anti-bugging devices should be used for discussion of material classified as TOP SECRET or SECRET. The BSI is to be consulted regarding the necessary
anti-bugging measures in good time before high-level or major conferences.

III. Discarding of classified material

26. Principles for the discarding of classified material

1. Material classified as CONFIDENTIAL or above which is no longer required should be discarded from the stock held by the department, for archiving or destruction in accordance with sections 27 and 28.

2. Approved cryptographic material (devices and keys) is to be discarded with the assistance of the BSI.

3. Material classified as RESTRICTED is to be discarded in the same way as unclassified material, under the Federal Archives Act. It should be destroyed in accordance with section 28.

4. When equipment is discarded for further, non-classified use, any classified material held in non-volatile memories within it (e.g. hard disks) is to be destroyed in accordance with section 28.

27. Archiving of classified material

1. Save where paragraph 3 applies, federal bodies are to offer any classified material which they no longer require to the Federal Archives (secret section) for archiving, in accordance with the Guidelines for the transfer of classified material to the secret section of the Federal Archives (Classified Material Archiving Guidelines, see Annex 8).

2. Federal authorities making use of the intermediate section of the Federal Archives, in accordance with section 20 of the Federal Government Registry Guidelines, should transfer any classified material which they no longer currently require to the Federal Archives (secret section) for further storage, in accordance with the Classified Material Archiving Guidelines.

3. Subordinate federal bodies with a regional remit for whose written material the archives of a Land are responsible, pursuant to section 2(3) of the Federal Archives Act of 6 January 1988 (BGBl. I, p. 62), as amended, are to offer any classified material which they no longer require to those Land archives (secret section) for archiving. The Classified Material Archiving Guidelines are applicable mutatis mutandis. Where there is no secret section, the classified material is to be kept by the body itself, until declassified.

4. Classified material in electronic form is to be offered for transfer to the Federal Archives, or in the cases referred to in paragraph 3 to the relevant Land archives, under the Classified Material Archiving Guidelines applied mutatis mutandis. The technical procedure for transfer is to be arranged with the archives beforehand.

28. Destruction of classified material

1. Any classified material not accepted by the relevant archives is to be destroyed in such a way as to make its contents unrecognisable and unreconstructable.

2. Material classified as CONFIDENTIAL or above may be destroyed only on the instructions of an authorised signatory working on classified material. The relevant classified material manager must check that the classified material is all there and destroy it in the presence of a suitably cleared witness.

3. The classified material register is to show on what date what classified material or part thereof was destroyed (for TOP SECRET and SECRET, giving the primary-copy number and number of pages) and who issued the instructions for its destruction. The note of this is to be signed by the classified material manager(s) involved and by the witness. If a classified material destruction record is drawn up, it will suffice for this to be signed by the classified material manager and the witness and referred to, giving its serial number, in the classified material register.

4. Unrecorded intermediate material for TOP SECRET material is to be destroyed by the relevant classified material managers, under the supervision of the person who produced it (or, for a transcript, the person who had it made and, for photocopies or printed copies, the person overseeing their making). Save as otherwise specified by
departmental heads, intermediate material for SECRET or CONFIDENTIAL material is to be passed to the relevant classified material managers for destruction, with no supervision being required.

5. Classified material on data carriers is to be erased using products approved by the BSI. If there are no approved products available, until they can be provided, ordinary commercial products developed for the purpose of secure erasure may be used. Where secure erasure is not electronically feasible (e.g. because of a defect), data carriers are to be physically destroyed in such a way that the information held on them cannot be reconstituted.

IV. Physical and technical measures

29. Area security measures

1. Classified material information technology rooms and other areas in which material classified as CONFIDENTIAL or above is processed in unencrypted form are to be protected from surreptitious unauthorised access.

2. Organisational units and individuals involved in managing, working on or otherwise dealing with classified material should, where possible, be located together.

3. With the consent of the relevant supreme federal authority, security areas should be established where necessary on account of the volume and significance of classified material. They are to be protected, by means of staffing, organisational and technical measures, from unauthorised access. Such areas must be accessible only at points at which reliable checks are made on access authorisation. Security areas may comprise individual or multiple rooms or entire buildings or complexes.

4. For classified material information technology rooms, the consent of the relevant supreme federal authority, in accordance with paragraph 3, can be taken for granted.

5. On entering a security area, those working in it are to be identified by means of their staff pass or in some other appropriate manner. After their identity has been established, visitors are to be kept under supervision while in the security area. Supervision may be dispensed with for visitors who can show (e.g. by means of a conference certificate in accordance with form 9 in Annex 3) that they have been screened under the Security Clearance Act and the general administrative instructions for security clearance. External personnel (workmen, cleaners, etc.) are to be screened in accordance with the Security Clearance Act and the general administrative instructions for security clearance and, where necessary, kept under supervision. In exceptional cases, supervision alone will suffice.

6. Staff carrying out checks are to be informed about all types of identification authorising access to the security area. Their tasks are to be spelt out in internal instructions. Visitor identification and other such records are to be kept for two years.

7. If a department has a security area in accordance with paragraph 3, discussion rooms with anti-bugging devices or that are bugging-proof (where necessary) should, as far as possible, be located within that security area.

30. Technical security of classified material

1. Technical means of protecting classified material must have been inspected by the BSI, to ensure that they fulfil the requirements in paragraph 2, and found suitable. The BSI may also agree to the use of other technical means in specific cases, provided they afford equivalent protection.

2. The following technical means of protecting classified material must meet the requirements set out below:

1) Classified material safekeeping facilities and key safes must be designed in such a way that:
   (a) access can be gained to their contents only after reliable identification and authentication by means of possession and knowledge; items possessed (e.g. keys) should be protected against unauthorised copying; biometric identifiers may also be used instead of or as well as possession and knowledge;
(b) any unauthorised access to their contents becomes apparent, and
(c) they are suitably protected against forcible access to their contents.

2) Alarm systems must be designed and installed in such a way that:

(a) they reliably detect any intruder;
(b) they cannot be disarmed by anyone unless that person has first been reliably identified and
 authenticated by means of possession and knowledge; biometric identifiers may also be used
 instead of or as well as possession and knowledge;
(c) the alarm is securely transmitted to the point where it is to be received, and
(d) the alarm system cannot be surreptitiously circumvented.

3) Classified material transport containers and packaging for letters or parcels must be designed in such a
 way that any unauthorised access to their contents becomes apparent.

4) Doors and locks or electronic access-control systems for rooms with anti-bugging devices or
 bugging-proof rooms or for access to any security areas not permanently manned must be designed in
 such a way that any unauthorised access becomes apparent; keys or other means of access must be
 protected against unauthorised copying.

3. The department must arrange for the technical means used in protecting classified material to be inspected by the
 BSI, in order to ensure proper implementation and detect any tampering; this is to be done as a rule when planning or
 first using classified material file security rooms or alarm systems for the protection of classified material and also in
 occasional spot checks or if any tampering is suspected. Paragraph 1 applies mutatis mutandis.

4. The necessary security measures are to be built into any restart arrangements for major information technology
 systems.

31. Guarding and technical surveillance of classified material

1. Guarding of the following requires the arrangements set out below:

1) for a classified material safekeeping facility: at least two people can directly, if within sight, or by means
 of technical aids, if out of sight, detect any attack and either avert it themselves (e.g. by force of arms) or
 report it immediately to security personnel who will come to the rescue;
2) for a building: multiple patrols are carried out at irregular intervals during a watch period or any attack
 can be detected by technical means and averted by security personnel.

2. Technical surveillance of the following requires the arrangements set out below:

1) for a classified material safekeeping facility: surveillance by means of an alarm system detecting any
 attack and reporting it immediately to security personnel who will come to the rescue;
2) for a building: surveillance by means of an alarm system detecting any unauthorised intrusion and
 reporting it immediately to security personnel who will come to the rescue.

3. Further details of the nature and extent of guarding and technical surveillance are to be decided by the security
 officer in the light of the protection sought for the classified material safekeeping facility or building in question.

32. Anti-bugging measures

1. The Federal Ministry of the Interior is to decide, in agreement with supreme federal authorities, which
 departments face a special bugging threat on account of the volume and significance of classified material and the tasks
 assigned them. In the case of departments referred to in section 45, a special bugging threat can be taken for granted.

2. Departments referred to in paragraph 1 must take precautions lest their telecommunications and information
 technology be improperly used to bug conversations conducted in rooms or by phone.
3. In departments referred to in paragraph 1, security officers must decide which rooms face a special bugging threat on account of the scale and significance of conversations conducted in them. For rooms in which conversations on matters classified as SECRET or TOP SECRET are conducted other than on an exceptional basis, a special bugging threat can be taken for granted.

4. Rooms referred to in paragraph 3 must be equipped with anti-bugging devices or bugging-proof. Such rooms must at least:
   
   1) be protected against surreptitious unauthorised access;
   2) possess acoustic attenuation adequately precluding any overhearing from outside without the use of technical aids;
   3) if equipped with telecommunications systems, have precautions taken so that conversations held in rooms cannot be listened in on via those systems;
   4) be designed in such a way (fittings, installations etc.) as to keep hiding places for bugging devices to a minimum and allow technical inspections in accordance with paragraph 5 to be carried out effectively, in a timely manner, and
   5) have precautions taken so that cables leading into rooms cannot be improperly used for bugging purposes.

Bugging-proof rooms are, in addition, to be designed in such a way as also to prevent any unauthorised transmission of conversations to the outside by means of technical aids (bugging devices).

5. In departments referred to in paragraph 1, technical inspections are to be carried out, upon completion of facilities and then at regular intervals or if any tampering is suspected, in order to ascertain whether:
   
   1) telecommunications or information technology systems can be improperly used for bugging purposes, or
   2) any bugging devices are present in the rooms referred to in paragraph 3, and
   3) the requirements of the technical guidelines referred to in paragraph 8 are fulfilled.

6. Technical inspections in accordance with paragraph 5 should also be carried out if bugging is suspected or at the time of any high-level or major conferences. In that event the extent of the inspection is to be arranged with the security officer or other organiser, depending on local circumstances at the time and the specific threat faced.

7. Departments must provide the requisite assistance for the technical inspections required under paragraphs 5 and 6.

8. In agreement with the Federal Ministry of the Interior, the BSI is to issue technical guidelines on security specifications for bugging-proof rooms or rooms with anti-bugging devices and for high-level or major conferences and on implementation of anti-bugging measures.

33. Safekeeping of keys and other others means of access to classified material

1. Keys for classified material safekeeping facilities, for classified material information technology rooms, for bugging-proof rooms or rooms with anti-bugging devices and for the arming or disarming of alarm systems for the technical protection of classified material are to be kept in staff's personal custody while at work, unless left in safekeeping in accordance with the second sentence. Before staff leave the building, keys should, as a rule, be locked away in a classified material safekeeping facility or key safe.

2. Classified material key safes should, as far as possible, be guarded. Where such a key safe is used by more than one individual, it must be fitted with lockable compartments in which users separately place their keys. This does not apply in the case of shared use of classified material safekeeping facilities or alarm systems. The keys to the lockable compartments are to remain in their users' personal custody.

3. Information technology systems used for classified material must have a reliable access control system, so that only authorised users are given access and can consult classified material, within the limits of their access rights. Repeated denials of access should result in the user being excluded from the system altogether. Such exclusion may be reversed only by the head of information technology security or someone acting on that head's instructions.

4. In assigning, amending or withdrawing rights, it must be ensured that:
1) the requisite request comes from an authorised source;
2) the person to be authorised has adequate security clearance;
3) the "need-to-know" principle is observed, and
4) functions are not combined where incompatible for security purposes.

Transfers of authority to assign and amend rights are to be documented and require security officers' consent. The documentation is to be kept for at least five years.

5. Use of physical means of access to information technology systems and components (magnetic cards, chip cards, dongles, punched tapes etc.) and details of the selection, assignment, verification and changing of passwords/personal identification numbers should be laid down in internal instructions.

34. Combination numbers as a means of access to classified material

1. The combination number for access to a classified material safekeeping facility or key safe or for the arming or disarming of an alarm system may be known only to users. It must not consist of easily discoverable numbers or groups of numbers, such as personal particulars, phone numbers or arithmetical series.

2. The combination number is to be written down and given to those who are to manage it, in a sealed envelope. Such envelopes are to be kept in at least the same way as material classified as CONFIDENTIAL. No other note of the combination number may be made.

3. Combination numbers for classified material safekeeping facilities or key safes or for the arming and disarming of alarm systems are to be changed:
   1) upon procurement;
   2) when users change;
   3) after any opening in users' absence;
   4) if unauthorised knowledge of the combination is suspected;
   5) at regular intervals of not more than twelve months.

Apart from users, changes may also be made by the relevant classified material managers, with security officers' consent, in the presence of the users.

4. Spare keys and notes of combination numbers are to be kept in labelled, sealed envelopes, in separate classified material safekeeping facilities (or, for spare keys, in classified material key safes). They are to be managed by different individuals, unless the managers in any case have access to the protected classified material (e.g. classified material managers and their deputies). Combination numbers for classified material key safes are to be kept and managed separately from those for classified material safekeeping facilities.

5. The preceding paragraphs are applicable mutatis mutandis to passwords, personal identification numbers and other combinations giving access to computers and electronic information technology used to process classified material. Further details are to be laid down in the departmental security plan.

35. Planning, procurement and acceptance testing

1. Departments using classified material other than on an occasional basis must draw up a combined plan for all security measures, in accordance with Annex 5, making allowance for specific departmental circumstances.

2. The necessary security precautions are to be taken in good time when planning and carrying out construction work. Further instructions are given in Annex 20/1 (Guidelines for security measures in construction work) to the Federal Construction Work Guidelines.

3. The BSI or, within the sphere of the Federal Ministry of Defence, the Military Counter-Intelligence Office is to be consulted over the planning and acceptance testing of classified material file security rooms, alarm systems for the
protection of classified material, telecommunications systems and bugging-proof rooms or rooms with anti-bugging devices.

4. If it is intended to make use of information technology for classified material, security officers and their information technology specialists are to be involved from the outset of planning. For complex information technology systems or special information technology applications for classified material, the BSI or, within the sphere of the Federal Ministry of Defence, the Military Counter-Intelligence Office should be consulted from the outset of planning.

5. In the procurement of information technology for use with classified material, procurement contracts are to specify the information technology security functions to be included in the system and the security specifications to be met by the producer or distributor. It must in particular be ensured that:

1) products with information technology security functions have received the necessary approval and are implemented in a manner consistent with security;
2) products with information technology functions are protected during storage and transport, as from the time at which it is known that they are to be used for classified material;
3) service and repairs are carried out in a manner consistent with security;
4) where information technology work is contracted out, the necessary security measures are taken.

V. Information technology measures

36. Authorisation and operation of information technology systems

1. Before information technology systems are first used for classified material, security officers must have them inspected to ascertain whether the necessary security measures have been taken. Security officers may call on the BSI for assistance; in the case of complex information technology systems or multiple information technology applications, the BSI should be consulted.

2. Classified material may be processed only on information technology systems confined to using hardware and software authorised by departmental heads. Such authorisation is to be documented.

3. Security-related changes to authorised information technology systems, particularly use for higher-classified material, require the prior consent of the relevant security officers, who are to follow the procedures in paragraphs 1 and 2 before any substantial changes.

4. Sections 4(3) and 18(2) are applicable mutatis mutandis to the operation of information technology systems.

37. Products with information technology security functions for use with classified material

1. Products having functions for:

1) production of key material;
2) encryption;
3) erasure or destruction of data carriers;
4) emanations security;
5) protection of transmission lines, or
6) separation of networks with different maximum classification levels for material processed,

must have been approved by the BSI. The approval must also include the necessary specifications concerning conditions of use and operation. Points 3 to 6 do not apply in the case of material classified as RESTRICTED.

2. Products having functions for:

1) system access control;
2) production of classified material;
3) logging or preservation of evidence and auditing;
4) prevention of tampering with information technology systems, or
5) registration and stock recording,
which are used for material classified as CONFIDENTIAL or above should have been approved by the BSI. Departmental heads may authorise the use of other products, especially if they are already in use or in the process of procurement at the time of entry into force of these instructions or if no suitable approved products are available and it is not possible to have any provided, or provided in time. Such other products include, in particular, products certified by the BSI in accordance with common criteria, using national protection profiles. Until national protection profiles become available, other BSI-certified products may also be used. The BSI procurement guide is to be used in selecting alternative products. Consultation of the BSI is advisable.

3. Approvals are to be ranked according to the need for protection of information technology applications for classified material, on the basis of generally accepted security criteria and procedures, which are to be supplemented by special attack-protection testing were necessary. Further details are to be set out by the BSI in an approval plan, to be endorsed by the Federal Ministry of the Interior.

4. Products with information technology security functions are, as from the time at which it is known that they are to be used for material classified as CONFIDENTIAL or above, to be:

1) stored in rooms referred to in section 29(1) or similarly protected areas;

2) transported under the constant supervision of staff cleared or approved in accordance with section 10(3) and (4), or packaged in such a way as to reveal any unauthorised access;

3) installed, serviced and repaired by staff cleared or approved in accordance with section 10(3) and (4), save where access to classified material is precluded by organisational measures (e.g. no processing or transmission of classified material in the presence of those concerned, who are kept under supervision), and

4) recorded in a register.

38. Emanations security

1. Information technology hardware holding material classified as CONFIDENTIAL or above in unencrypted form should be installed in accordance with BSI emanations security guidance.

2. Security officers are to consider, in accordance with BSI guidance, and departmental heads to decide to what extent unauthorised utilisation of compromising emanations can be expected to pose a significant threat to the security of material classified as CONFIDENTIAL or above. Where a significant threat is likely, the information technology hardware must be operated in BSI-approved emanation-proof rooms, have received BSI approval for operation within a specified security zone (under the zoning system) and be operated within such a zone or else have been approved by the BSI as emanation-proof.

39. Technical testing

1. Where information technology systems are used for TOP SECRET material, or for SECRET material other than on an exceptional basis, before they are first used for classified material and at appropriate intervals thereafter, security officers must have the following technical tests carried out by the BSI:

1) testing of the information technology system under its specific conditions of use, to see whether the necessary information technology security functions have been properly implemented, show no signs of tampering and, once implemented, operate effectively in that system, cannot be tampered with or circumvented via the system and also display such security if connected to any other information technology systems;

2) tests for emanations security and to detect tampering in emanation-proof rooms or containers, in zoned rooms and on hardware used for classified material, and

3) inspection of security zones to detect any equipment for the recording or transmission of compromising close-range emanations.
2. The BSI is to notify security officers of the test results in test reports.

3. Where networked information technology systems are used for classified material in departments referred to in section 5(3), security officers are to have a penetration test carried out.

40. Transmission of classified material via telecommunications or other technical communications systems

1. When transmitted via telecommunications or other technical communications systems, classified material is to be encrypted, using a cryptographic system approved by the BSI for the relevant classification level, or protected by some other approved means. Where no BSI-approved programmes and equipment are available for use with material classified as RESTRICTED, use may also be made of products certified by the BSI in accordance with common criteria, using national protection profiles. Until national protection profiles become available, use may be made of other BSI-certified products, tested to at least EAL 3 standard. The BSI procurement guide is to be used in selecting certified products.

2. Notwithstanding the first sentence of paragraph 1, unencrypted transmission may be used in the following cases:

1) if the matter to be dealt with is urgent and transmission in writing or by other secure means would cause undue delay, use may be made:
   (a) for phone calls on matters classified as CONFIDENTIAL, of a line approved for RESTRICTED material in accordance with the first sentence of paragraph 1, and
   (b) for phone calls on matters classified as RESTRICTED, of an unprotected line.
   Conversations should, as far as possible, be conducted in such a way that the matter discussed cannot be understood by any outsider. If the identity of the person at the other end is in any doubt, a new call must be made as a check. Particular care should be taken with radiotelephone (e.g. mobile, DECT10 or bluetooth11) calls;

2) for urgent e-mails, faxes or telexes classified as RESTRICTED, if the sender and recipient do not have any encryption facility or other means of protection (such as a password) for the requisite mode of transmission. Before sending the message, the sender must ensure by appropriate means that it reaches the rightful recipient;

3) in exceptional cases, with the consent of the departmental head or, for authorities referred to in the first sentence of section 5(3), of the division or section head, in addition to the above exceptions, for transmission of material classified as CONFIDENTIAL or SECRET (provided it is not marked for any special classified treatment, such as cryptography), if:
   (a) the sender and recipient do not have any encryption facility, and
   (b) the classified material cannot be conveyed in time by other means and any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material.

Messages should, as far as possible, be worded in such a way as to avoid making their classified nature immediately apparent. They must not show any markings or indications distinguishing them from an unclassified message. Their recipients are to be notified of the message classification level, without delay, by other means (e.g. other telecommunications systems, mail or courier), save where this is not possible or appropriate in any particular case.

3. In transmitting classified material, in addition to the exceptions laid down in paragraph 2, encryption may be dispensed with:

1) within an access-controlled information technology room;
2) if the transmission facilities are protected in such a way as to make any unauthorised access immediately apparent (approved circuits12), or

3) if, within a departmental network:
   (a) RESTRICTED material is transmitted;
   (b) only CONFIDENTIAL or, in exceptional cases, SECRET material is transmitted;
   (c) an access control system in accordance with section 37(2) is in place, and
   (d) the transmission facilities are entirely enclosed within an area with reliable access control or, where not so enclosed, are protected against direct unauthorised access;

where the network is connected to another communications network, that other network and the connection with it must be protected at least in accordance with (c) and (d).

4. Where the cryptographic (key) material required for the operation of a cryptographic system is not generated automatically, it may be produced and distributed only by the BSI or by BSI-designated sources; Cryptography managers and deputies are to be appointed, to deal with cryptographic material supplied by courier or mail. Cryptography managers are to enter cryptographic material in cryptographic systems or, if need be, issue it to authorised information technology users. The names and office addresses of cryptography managers and their deputies and any changes in them are to be notified to the BSI or to BSI-designated bodies.

5. Security specifications for telecommunications systems used to discuss matters classified as CONFIDENTIAL or above in unencrypted form are to be laid down in technical guidelines issued by the BSI, in agreement with the Federal Ministry of the Interior.

6. In communications with foreign or international bodies (e.g. NATO), the relevant international rules and agreements take precedence, save where domestic rules require more stringent security measures.

41. Servicing and repair of information technology for material classified as CONFIDENTIAL or above

1. Such classified material is to be removed from the information technology system prior to any servicing or repair work. Should that not be possible, service or repair staff cleared or approved in accordance with section 10(3) and (4) are to be used. Servicing or repair work may not normally be carried out on an information technology system while classified material is being processed or transmitted.

2. Remote servicing is permissible only if:
   1) it is carried out by staff cleared or approved in accordance with section 10(3) and (4);
   2) cryptographic systems are used for transmission in the course of remote servicing;
   3) reliable access control, preservation of evidence and auditing are in place, and
   4) each remote servicing procedure is separately launched and terminated by the department.

Remote servicing should be carried out only when no classified material is being worked on and all classified data accessible in the information technology system have been encrypted or erased.

3. Notwithstanding paragraph 2, security officers may allow a firm to carry out remote servicing if:
   1) security guidance concerning the firm has been received from the Federal Ministry of Economic Affairs and Technology, or another supreme federal authority has ensured that the necessary security measures are in place at the firm;
   2) each remote servicing procedure is separately launched and terminated by the department and is monitored by it;
3) the procedures in points 2 and 3 of the first subparagraph and in the second subparagraph of paragraph 2 are followed;

4) a contract or contract rider concerning the necessary security measures has first been concluded with the firm.

4. Where any classified material information technology leaves the department (e.g. because of a defect or at the end of a leasing agreement), classified material held on data carriers inside it is to be erased, using BSI-approved equipment or programmes. Should that not be possible, the data carriers are to be removed and physically destroyed in such a way that the information held on them cannot be reconstituted.

VI. Concluding provisions

42. Inspections

1. In every department using classified material, unannounced spot-check inspections are to be carried out, at appropriate intervals, to ascertain whether:

   1) classified material produced there has clearly been unjustifiably or incorrectly classified; if in doubt, reasons in writing may be sought from the issuer;

   2) the classified material held is being dealt with in accordance with the Classified Material Instructions.

Inspections are to be carried out by security officers or by specially designated members of staff, such as security personnel.

2. All staff must assist in the carrying out of inspections and allow access to any classified material, upon request, for the purpose.

3. The security officers or specially designated members of staff are to check in particular on the nature and scale of measures for the protection of material classified as CONFIDENTIAL or above, in order to ascertain whether:

   1) clearance for access to classified material and approval for work in accordance with section 10(4) are necessary to the existing extent;

   2) those cleared for access to classified material or approved for work in accordance with section 10(4) have been adequately screened and informed about the security rules to be observed;

   3) classified material is properly produced, reproduced, marked, recorded, stored and circulated and any no longer required is properly destroyed or transferred to the secret section of the Federal Archives;

   4) the "need-to-know" principle is adequately observed in practice.

4. Heads of information technology security are in particular to check whether:

   1) information technology security components are being used, serviced and repaired in a manner consistent with security;

   2) access rights, as granted, have been correctly assigned and are necessary;

   3) means of identification or authentication are properly protected;

   4) the hardware and software authorised has not been changed.

5. Data logged in preserving evidence are to be regularly audited to ascertain:

   1) any denials of access, and
2) any clearly illegitimate access to classified data.

6. A record is to be made of inspections and of any findings of relevance to security. The record is to be kept for five years.

43. Reporting of any breach of security to security officers

Security officers are to be notified without delay if it is discovered or suspected that:

1) any classified material has come to the knowledge of anyone unauthorised, or any cryptographic keys needed for decryption of classified material or other means of access to classified material have come to the knowledge of anyone unauthorised or been lost;

2) any classified material or any key for a classified material safekeeping facility, for a lockable compartment in a classified material key safe or for the arming and disarming of an alarm system has been lost;

3) any security rules have been broken, or

4) any other circumstances have a bearing on security (e.g. security installations are defective or particular individuals show an unusual interest in classified material).

44. Response to any breach of security or discovery of a security vulnerability

1. In the event of any breach of security or discovery of a security vulnerability, security officers are to establish the facts of the matter. They must take the necessary action to prevent or reduce any harm and avoid any recurrence. If initial investigations show that intelligence service involvement or a treasonable act of any other kind cannot be ruled out, the Federal Office for the Protection of the Constitution or, within the sphere of the Federal Ministry of Defence, the Military Counter-Intelligence Office is to be brought in.

2. If any material classified as CONFIDENTIAL or above has or may have come to the knowledge of anyone unauthorised, the issuing body is to be informed and referred to these instructions. The issuing body must take the measures necessary, for its part, to prevent or reduce any harm (e.g. by changing its plans or intentions and notifying any others involved). Where there is any German classified material of considerable significance or non-German classified material involved, the Federal Ministry of the Interior, as the national security authority, is to be informed without delay.

3. If any means of access (such as passwords or chip cards) to electronic information technology used for classified material or any keys for a classified material safekeeping facility, for a lockable compartment in a classified material key safe or for the arming and disarming of an alarm system are lost, or if there is reason to believe that anyone unauthorised may have obtained or be able to obtain access to classified material by tampering with security components, the means of access or keys are to be replaced with new ones or the use of information technology is to be restricted or suspended.

4. Where the Federal Office for the Protection of the Constitution has been brought in following an incident, under paragraph 1, it is to report its findings to the head of the relevant department without delay. The departmental head must take any further action required.

5. Even if not incurring prosecution under the Criminal Code, breaches of the Classified Material Instructions may entail disciplinary penalties or employment action (including dismissal).
45. Special departments

1. Departments identified by the Federal Ministry of the Interior as being especially exposed to attacks on the confidentiality, integrity and availability of classified material are to take further security precautions, in cooperation with the BSI. These include in particular:

   1) intensive briefing of their staff;
   2) appointment of their security officer and training of that officer by the BSI, in order to tighten up checks;
   3) more frequent spot-check inspections; where necessary, the BSI is to provide advice and technical assistance;
   4) regular extensive counselling by the BSI (at least every four years);
   5) establishment of security areas;
   6) installation of bugging-proof rooms or, as a minimum, rooms with anti-bugging devices;
   7) precautions against unauthorised reproduction of material classified as CONFIDENTIAL or above.

2. Within its sphere, the Federal Ministry of Defence is to identify departments covered by paragraph 1 itself, where the Military Counter-Intelligence Office will replace the BSI for these purposes.

3. In such departments, technical tests are to be carried out in accordance with section 39 and anti-bugging measures taken in accordance with section 32 at least every four years. Inspection of rooms should cover rooms with anti-bugging devices and bugging-proof rooms as well as other rooms at risk from bugging for any particular reason (e.g. international conferences). Information technology and telecommunications systems are to be inspected, in particular to ascertain whether they incorporate the necessary security precautions and, as each configured, do not leave any unauthorised functions active.

46. Final provisions

1. If, in the event of a disaster or an alarm and evasive action, there is a risk of unauthorised access to material classified as CONFIDENTIAL or above, the classified material is to be protected or destroyed.

2. The Federal Ministry of the Interior may, in liaison with supreme federal authorities, amend the Classified Material Instructions and supplement them with advice and guidelines.

3. Any department may go beyond the Classified Material Instructions and take more stringent security precautions, provided they do not disrupt the necessary uniform treatment of classified material throughout the system for dealing with it.

4. In particular special cases, the Federal Ministry of the Interior may also agree to other exceptions, provided the protection to be provided by the Classified Material Instructions is achieved by means of other security precautions.

5. Where any of the Classified Material Instructions cannot be applied at German missions abroad, the Ministry of Foreign Affairs is to decide, in agreement with the Federal Ministry of the Interior, on the procedure to be followed.

6. The Federal Intelligence Service may, with the consent of the Federal Chancellery, issue rules for its sphere which differ from the Classified Material Instructions.

7. The Federal Ministry of Defence is to deal with the treatment of classified material within its sphere by means of central internal rules consistent with the Classified Material Instructions.

8. The German Parliament is to deal with security matters on its own behalf.
47. Entry into force and repeal

These General Administrative Instructions and the annexes to them are to enter into force on 1 June 2006. The General
Administrative Instructions for the physical and organisational protection of classified material (Classified Material
Instructions) issued by the Federal Ministry of the Interior on 29 April 1994 (GMBl. [joint ministerial gazette] 1994,
p. 674), as last amended by the First Classified Material Instructions Amending Administrative Instructions of
1 July 2001, are hereby repealed, as are the following guidelines issued under them:
− Guidelines for the security of classified material in the use of information technology (Classified Material
Information Technology Guidelines) of 1 September 1998;
− Guidelines for advice and inspection for the protection of classified material (Classified Material Inspection
Guidelines) of 1 September 1998;
− Guidelines for the transfer of classified material to the secret section of the Federal Archives (Classified Material
Archiving Guidelines) of 20 March 1991;
− Guidelines for the technical protection and guarding of classified material (Classified Material Protection
Guidelines) of 1 September 1998.

The following annexes to these instructions are applicable:

Annex 1: Classification guidance
Annex 2: Marking guidance and examples
Annex 3: Guidance and forms for recording classified material
Annex 4: Guidance for the marking of non-German classified material
Annex 5: Guidance for classified material documentation
Annex 6: Guidance for the transfer and dispatch of classified material
Annex 7: Guidance for the handling of material classified as RESTRICTED
Annex 8: Classified material archiving guidelines

Berlin, 31 March 2006

Dr Dürig

Definitions

Terms used are explained only if they are employed with a special meaning for classified material or not commonly met
with in administrative practice.

1) Availability of classified material
   Authorised access must be ensured, e.g. by depositing a spare key or making back-up copies of electronic
   material.

2) Integrity (or intactness) of classified material
   Certainty that classified material is all there and has not been altered, e.g. by having an attachment removed.
   This can happen as a result of inadequate protection (such as an ordinary lock).

3) Electronic signature
   The integrity of electronic files can be checked by cryptographic means. Further details are given in the Digital
   Signatures Act and rules issued under it.

4) Data carrier
A storage medium for computer data and software, such as diskettes, hard disks or CDs.

(5) **PDA**
Personal digital assistant: a portable microcomputer.

(6) **Non-volatile memory**
A distinction is made between memories which lose the data held in them when switched off (mostly used inside equipment) and non-volatile memories, which retain their contents at least until next used (e.g. diskettes, CDs or hard disks).

(7) **Dongle**
A device for computers, usually in plug-in form, to protect functions, such as copying or access.

(8) **Common criteria**
A procedure for confirming (certifying) the security of computer systems and of their components. On the basis of testing by an independent body, an official certificate confirms that the product provides the required standard of protection.

(9) **Penetration test**
A procedure for testing the protection of a computer network against unauthorised hacking into computers connected to it.

(10) **DECT**
Digital European cordless telecommunications: a standard for phones using cordless handsets (by radio), but working only with a particular landline connection.

(11) **Bluetooth**
A procedure for connecting up electronic appliances by radio, e.g. hands-free devices for mobile phones.

(12) **Approved circuits**
Circuitry protected by special means in such a way as to reveal any unauthorised access ("tapping").
Annex 1 to the
Classified Material (CM) Instructions

Classification Guidance

1. General Points

Through judicious and appropriate classification, help to ensure that
– information which really does need to be classified is protected effectively, and
– unnecessary security costs are avoided.

The security level of an item of CM depends on its content and not on the security level of the process in which it is involved or to which it relates. A document with CM Annexes is to be classified at a level which is at least as high as that of the Annex with the highest classification. If a document is classified or is classified at a higher level on the basis of its Annexes, it should bear a note to the effect that without the Annexes it is no longer to be treated as CM or is to be classified at a lower level.

Within the overall classification of an item of CM, clearly identifiable parts, e.g. parts of plans, sections, chapters, lists or numbers, may be classified at a lower level or not at all.

Make a critical assessment of whether classification is really necessary.

There should in particular be an assessment of whether the need for protection through classification only obtains for a limited time (see section 9(2) of the CM Instructions).

For classification, there must be conclusive demonstration of the concrete risks, harm or detriment to the Federal Republic of Germany or one of its Länder which may arise if unauthorised persons obtain knowledge of the information.

Moreover, classification may in principle only be envisaged in the case of information concerning
– external security,
– external relations, or
– internal security,
– third-party interests to be protected by the Federal Republic of Germany.

In the case of other information requiring protection, use should be made of the relevant existing regulations (e.g. obligation to keep official or tax secrets, protection of personal data under the Data Protection Act, Federal Archive Act or internal rules of procedure).

Any classification as CONFIDENTIAL or above means that all persons dealing with such information must undergo a costly security check intruding on personal rights and that cost-intensive practical measures to protect the CM must be
taken. For classification, the chosen security level and the protection measures involved must reflect the concrete need for protection.

2. Classification Examples

2.1. Classification as TOP SECRET can be envisaged *inter alia* for

- parts of the Federal Armed Forces' alarm plan,
- information generated by the Federal Intelligence Service,
- other compilations, the elements of which are classified as SECRET but which should be given the overall classification of TOP SECRET.

2.2. Classification as SECRET can be envisaged *inter alia* for

- information on the Federal Armed Forces' "electronic campaign"
- parts of the Federal Armed Forces' alarm plan,
- documentation concerning critical infrastructures,
- State and other important treaties of the Federal Republic of Germany,
- cryptodata used for the encryption of material that is given a CONFIDENTIAL or higher classification,
- compilations, the elements of which are classified as CONFIDENTIAL but which should be given the overall classification of SECRET.

2.3. Classification as CONFIDENTIAL can be envisaged *inter alia* for

- investigation reports in suspected espionage cases,
- findings concerning the working methods of extremist/terrorist organisations, disclosure of which would jeopardise further observation/reconnaissance,
- foreign-policy negotiating positions, premature revelation of which would be to the detriment of German interests,
- documentation concerning critical infrastructures,
- State and other important treaties of the Federal Republic of Germany,
- important inventions, commercial and company secrets or other private facts, matters or findings, knowledge of which by unauthorised persons may harm the Federal Republic of Germany,
- plans of the computer networks and configuration data of the systems used by departments referred to in section 5(3) of the CM Instructions,
- compilations, the elements of which are classified as RESTRICTED but which should be given the overall classification of CONFIDENTIAL.
These may *inter alia* be

- computer networks where various processors occasionally process RESTRICTED CM. Although even in a larger department there are only a few items of CM at any given workstation, on the servers the compilation can absorb such a vast range of information that a breach of confidentiality may well harm the Federal Republic or one of its Länder. The interface for classification is accordingly the network upstream of the circuits of the individual workstation computers.

- compilations of police investigations which are not individually classified or are classified as RESTRICTED but which overall reveal police procedures.

**2.4. Classification as RESTRICTED can be envisaged *inter alia* for**

- final reports on security checks on persons,
- search documentation in the fields of terrorism/extremism,
- compilations concerning security-system measures (security-system documentation),
- special internal instructions and duty rosters,
- records of computer networks of the departments referred to in to section 5(3) of the CM Instructions,
- compilations of police investigations which are not individually classified but which overall reveal police procedures.
Annex 2 to the CM Instructions

Marking Guidance and Examples

N.B. The following guidance applies chiefly to documents. For other forms of CM, comparable protective measures should be taken.

1. General Points

1.1. In the case of material classified as TOP SECRET or SECRET, the classification is stamped or printed in red at the top and bottom of every written page together with the words "officially classified". The written pages must be numbered; the total number of such pages must be indicated on the first page. The CM must be given a reference number and date. The reference number must be accompanied at the end by the abbreviation "top secr." or "secr."; in the case of material classified as TOP SECRET, this must be done on every written page.

1.2. In the case of material classified as CONFIDENTIAL, the classification is stamped, printed or typewritten in black or blue at the top of every written page together with the words "officially classified". The written pages must be numbered. The CM must be given a reference number and date. The reference number must be accompanied at the end by the abbreviation "conf."

1.3. In the case of material classified as RESTRICTED, the classification is stamped, printed or typewritten in black or blue at the top of every written page. The CM must be given a reference number and date. The reference number must be accompanied at the end by the abbreviation "restr.". In the case of books, brochures and the like, marking on the cover and title page is sufficient.

1.4. The outer front and back pages and, where appropriate, the backs of document containers (circulation, self-adhesive cover and other folders, loose-leaf and other binders) in which CM classified as TOP SECRET, SECRET or CONFIDENTIAL is sent or kept must be marked as follows:

1) in the case of TOP SECRET, with crossed diagonal stripes (one yellow and one red),
2) in the case of SECRET, with a red diagonal stripe,
3) in the case of CONFIDENTIAL, with a blue diagonal stripe.

CM transport containers are exempted from such external marking.

1.5. CM registers must be marked in the same way.

1.6. In the case of cryptographic systems, classified cryptographic (key) material required for encryption and decoding, descriptions, components and other documentation may irrespective of the security level be marked with the warning CRYPTO in order to facilitate application of the "need-to-know" principle.

2. Examples

The following examples are simply suggestions and in implementing the rules to be applied in the various departments, the determining factor is the content of the texts.

Example 1  Final draft of an item of CM that is TOP SECRET

Example 1a  Primary copy of an item of CM that is TOP SECRET
Example 1b  **Template** of a standard letter that is TOP SECRET

Example 1c  **First primary copy** of a standard letter that is TOP SECRET as exemplified in 1b

Example 2  **Final draft** of an item of CM that is SECRET

Example 2a  **Primary copy** of an item of CM that is SECRET

Example 2b  **Annex** to an item of CM that is SECRET

Example 3  **Final draft** of an item of CM that is CONFIDENTIAL

Example 3a  **Primary copy** of an item of CM that is CONFIDENTIAL

Example 4  **Final draft** of an item of CM that is RESTRICTED

Example 5  **Item of CM the parts of which are classified at different levels**

Example 6  **Authorisation and endorsement of reproductions (e.g. copies)**

Example 6a  **Copy** of an item of CM that is SECRET

Example 6b  **Copy of a copy** of an item of CM that is SECRET

Example 7  **Envelopes for sending CM** (here: SECRET)

Example 8  **Marking for CM data carriers** (here: CD-ROM)

Example 9  **Marking of the cover for CM data carriers** (here: CD-ROM)

Example 10  **Marking for CM data carriers** (here: USB Stick)
Final draft
of an item of CM that is "STRENG GEHEIM" ("TOP SECRET")

Specification of the number of primary copies (without final draft) to be produced and their recipients

Date

Reference number with abbreviation of the classification on the first page

Initials of the person producing the CM (e.g. typist, techn. draughtsman)

Indication of the total number of written pages on the first page

Classification together with the words "Amtlich geheimgehalten" ("officially classified") stamped or printed in red at the top and bottom of every written page

(*) Collective addresses omitting "z.Hd. Herrn" ("att. Mr...") in the cover note (e.g. by addition of a distributor to the final draft) are permitted. It must however be clear who has received which primary-copy number. This does not affect the way the address (Example 7) appears on the envelope.
Example 1

Reference number with abbreviation of the classification on every written page

Numbering of the written pages

Classification together with the words "Amtlich geheimgehalten" ("officially classified") stamped or printed in red at the top and bottom of every written page
Example 1a

**Primary copy**
of an item of CM that is "STRENG GEHEIM" ("TOP SECRET")

- **Primary-copy number on the first page**
- **Date**
- **Reference number with abbreviation of the classification on the first page**
- **Indication of the total number of written pages on the first page**
- **Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in red at the top and bottom of every written page**
Example 1a

Reference number with abbreviation of the classification on every written page

Numbering of the written pages

Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in red at the top and bottom of every written page
Template

of a standard letter that is "STRENG GEHEIM" ("TOP SECRET")

Standard print areas
(column headings of
the data source)

Other areas as in
Example 1

Final-draft version is
printed only if the
print option "hidden
text" is activated
Example 1b

Standard print areas
(column heading of the
data source)

Numbering of the written
pages

Classification together
with the words "amtlich
geheimgehalten"
("officially classified")
stamped or printed in red
at the top and bottom of
every written page
Example 1b

Column headings of the word table give the standard print areas

File numbers must be entered in every data set (can be copied)
**Example 1c**

**Primary copy**

First printout of a standard letter (as exemplified in 1b)

From standard print areas

Other areas as in Example 1

Final-draft version is also printed only if the print option "hidden text" is activated
Example 1c

From standard print area

Numbering of the written pages

Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in red at the top and bottom of every written page.
Example 2

Final draft

of an item of CM that is "GEHEIM" ("SECRET")

Specification of the number of primary copies (without final draft) to be produced and their recipients

Date

Reference number with abbreviation of the classification on the first page

Initials of the person producing the CM (e.g. typist, techn. draughtsman)

Note that the document without Annexes is not classified

Note of the Annex(es)

Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in red at the top and bottom of every written page

(*) Collective addresses omitting "z.Hd. Herrn" ("att. Mr...") in the cover note (e.g. by addition of a distributor to the final draft) are permitted. It must however be clear who has received which primary-copy number. This does not affect the way the address (Example 7) appears on the envelope.
Example 2

Reference number with abbreviation of the classification on the first page

Numbering of the written pages

Classification together with the words "Amtlich geheimgehalten" ("officially classified") stamped or printed in red at the top and bottom of every written page
Example 2a

Primary copy

of an item of CM that is "GEHEIM" ("SECRET")

Primary-copy number on the first page

Date

Reference number with abbreviation of the classification on the first page

Note that the document without Annexes is not classified

Indication of the total number of written pages on the first page

Note of the Annex(es)

Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in red at the top and bottom of every written page
Example 2a

Reference number with abbreviation of the classification on the first page.

Numbering of the written pages.

Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in red at the top and bottom of every written page.
Example 2b

Annex
to an item of CM that is "GEHEIM" ("SECRET")

Indication of the CM (issuing department, reference number, date and primary-copy number) to which the Annex belongs

N.B.

If the CM is re-circulated, the details may be retained provided this is pointed out in the (new) cover note
Example 3

Final draft

of an item of CM that is "VS-VERTRAULICH" ("CONFIDENTIAL")

Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in black or blue at the top of every written page

Date

Reference number with abbreviation of the classification on the first page

Initials of the person producing the document (e.g. typist, techn. draughtsman)

Specification of the number of primary copies (without final draft) to be produced and their recipients

Stipulation of the date from which the classification is no longer necessary or is not necessary to the same extent (section 9(2))

(*) Collective addresses omitting "z.Hd. Herrn" ("att. Mr...") in the cover note (e.g. by addition of a distributor to the final draft) are permitted. It must however be clear who has received which primary-copy number. This does not affect the way the address (Example 7) appears on the envelope.
Example 3

Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in black or blue at the top of every written page

Numbering of the written pages
Example 3a

Primary copy

of an item of CM that is "VS-VERTRAULICH" ("CONFIDENTIAL")

Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in black or blue at the top of every written page

Date

Reference number with abbreviation of the classification on the first page

Stipulation of the date from which the classification is no longer necessary or is not necessary to the same extent (section 9(2))
Example 3a

Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in black or blue at the top of every written page

Numbering of the written pages
Example 4

Final draft

of an item of CM that is "VS-NUR FÜR DEN DIENSTGEBRAUCH" ("RESTRICTED")

Classification together with the words "amtlich geheimgehalten" ("officially classified") stamped or printed in black or blue at the top of every written page

Date

Reference number with abbreviation of the classification on the first page
Example 5

Item of CM parts of which are classified at different levels

Indication that individual parts of the CM are classified at different levels

Beginning and end of the parts classified at different levels must be clearly shown (e.g. by lines or numbering)

N.B.
If individual parts are to be transmitted or kept separately (e.g. parts of plans), the individual parts should be marked as Annexes and recorded in the cover note. In the absence of a cover note, a cover sheet should be prepared instead indicating the overall classification and recording the Annexes individually.
Example 6

Authorisation and endorsement of reproductions (e.g. copies)

The copies have been authorised and endorsed on the blank back of the page to ensure that the authorisation and endorsement are not also copied.
Copy of an item of CM that is "GEHEIM" ("SECRET")

1. Ausfertigung 6. Kopie

GEHEIM
amtlich geheimgehalten

BUNDESAMT FÜR VERFASSUNGSSCHUTZ
Köln, den 20.2.1994

5 Seiten

Bundesministerium des Innern
z.Hd. Herrn MinDir Großmann
- oViA-
Graurheindorfer. Str. 198
53117 Bonn

Herrn Minister
über
Herrn St S

mit der Bitte um Kenntnisnahme vorgelegt.

(Großmann)

Betr.: - Text -
Bezug: - Text -

- Text -
Example 6b

Copy
of a "GEHEIM" ("SECRET") copy
(e.g. an authority makes a further copy on receipt from the Federal Ministry of the Interior of the fourth copy of the first primary copy of a communication from the Federal Office for the Protection of the Constitution)

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GEHEIM GEHEIM GEHEIM</td>
</tr>
<tr>
<td>amtlich geheimgehalten</td>
</tr>
<tr>
<td>amtlich geheimgehalten</td>
</tr>
<tr>
<td>amtlich geheimgehalten</td>
</tr>
</tbody>
</table>

BUNDESAMT FÜR VERFASSUNGSSCHUTZ
Köln, den 20.2.1994

5 Seiten

Bundesministerium des Innern
z.Hd. Herrn MinDir Großmann -oViA-
Graurheindorfer. Str. 198
53117 Bonn

Betr.: - Text -
Bezug: - Text -

GEHEIM GEHEIM GEHEIM
amtlich geheimgehalten          |
amtlich geheimgehalten           |
amtlich geheimgehalten           |

Each reproduction is given a serial number
Marking stamped or printed in red (re-stamped)
Example 7

Envelopes for dispatching CM (here "GEHEIM"/"SECRET")

– outer envelopes –

**By courier**

When a courier is used either the reference number without classification or a source number must be given (done by CM registry)

Bayerisches Staatsministerium des Innern
z.Hd. Herrn MinR Dr. Huber -oViA-
Odeonsplatz 3
80539 München

151/71
(oder/or)
3233

**By private delivery service**

Address of the department with indication of the authorised recipient (position or name) together with "oViA" ("or his representative")

Bayerisches Staatsministerium des Innern
z.Hd. Herrn MinR Dr. Huber -oViA-
Odeonsplatz 3
80539 München
Example 8

Marking for CM data carrier (CD-ROM)

[CONFIDENTIAL officially classified CM data carrier]

[SECRET officially classified CM data carrier]
Example 9

Marking of the cover for CM data carriers (CD-ROM)

[CONFIDENTIAL officially classified CM data carrier]

[SECRET officially classified CM data carrier]
Example 9

Marking of the cover for CM data carriers (CD-ROM)

[TOP SECRET officially classified CM data carrier]
Example 10

Marking for CM data carriers (USB sticks)

[CONFIDENTIAL officially classified]

Recto

VS-VERTRAULICH
amtlich geheimgehalten

Verso

[CM data carrier]

Tgb.- Nr.: VS-Datenträger
Nr.: V353

[SECRET officially classified]

Recto

GEHEIM
amtlich geheimgehalten

[TOP SECRET officially classified]

STRENG GEHEIM
amtlich geheimgehalten

Verso

(TM SECRET)

Tgb.- Nr.: VS-Datenträger
Nr.: G374

[CM data carrier]
Annex 3 to the CM Instructions

Guidance and Forms for Recording CM

Guidance for keeping CM registers

N.B. The following guidance applies chiefly to documents. For other forms of CM comparable protective measures should be taken.

In keeping CM registers, the department managing the CM may diverge from form 10 but the following are to be taken into account:

1. The first page should contain a note of the classification levels being recorded and the name of the person who is responsible for keeping the CM register.

2. The pages of bound CM registers should be numbered. Where CM registers are in the form of card files, the files are to be numbered continuously and marked with an official seal. Where CM registers are in electronic format and in loose-leaf form, the Federal Office for Information Security should be consulted.

3. CM registers are allocated the classification level of the CM recorded in them; exceptions in individual cases require the consent of the security officer. In the case of mobile data carriers and bound documents, the marking is to be placed on the item, the cover or the title page. In the case of filing cards or loose-leaf pages, the marking should be applied to each card individually.

4. In the CM registers every receipt, dispatch, location, reproduction, downgrading and destruction of material classified as TOP SECRET, SECRET or CONFIDENTIAL should be recorded and special deadlines for withdrawing or downgrading the classification should be noted.

5. Material classified as TOP SECRET should be kept in a separate CM register.

6. Each item of CM should be recorded in the CM register under its own serial number. If further items received are registered under the same number as an item of CM already recorded, material classified as TOP SECRET or SECRET should be allocated an additional number as a distinguishing feature (e.g. exponent or batch).

7. Entries should be made in ink or biro (permanent in accordance with DIN standard 16554). Alterations must be clearly shown with date and signature. Any deletions must leave the original text legible. In CM registers there must be no erasures, rendering entries indecipherable or removal or addition of pages. Where entries are not permanently required (e.g. deadlines for re-submission), the security officers may allow exceptions after consulting the Federal Office for Information Security.

8. The CM administrators should confirm receipt of new CM registers (CM logs or cards). The security officers or persons authorised by them should take charge of the receipt certificates and any CM transfer discussions.

Record forms

The forms are also made available electronically as a template.

Form 1 Obligation to ensure the security of classified material
Form 2 Clearance and approval
Form 3 Repeat notification
Form 4 Withdrawal of clearance or approval
Form 5 CM accompanying note
<table>
<thead>
<tr>
<th>Form 6</th>
<th>CM transfer record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form 7</td>
<td>CM destruction record</td>
</tr>
<tr>
<td>Form 8</td>
<td>CM receipt form</td>
</tr>
<tr>
<td>Form 8d</td>
<td>CM exchange</td>
</tr>
<tr>
<td>Form 8e</td>
<td>CM exchange</td>
</tr>
<tr>
<td>Form 9</td>
<td>Conference certificate</td>
</tr>
<tr>
<td>Form 10</td>
<td>CM register</td>
</tr>
<tr>
<td>Form 11</td>
<td>Receipt book</td>
</tr>
</tbody>
</table>
in connection with the intended communication of an officially classified matter (classified material), had his/her attention drawn today to the provisions of sections 93 to 99 and 353 b (2) and (3) of the Criminal Code. He/she was informed of the relevant provisions concerning the protection of classified material.

He/she was informed, inter alia, that:

1. records and notes may be made only with the express permission of the discussion partner/negotiator and are not to be made accessible to any unauthorised persons.

2. he/she is responsible for the safekeeping of the classified material handed over as well as for ensuring that its content is not made accessible to unauthorised persons.

3. any kind of reproduction of classified material and the production of extracts is prohibited.

Mr/Mrs/Ms

Name, first name

is accordingly formally bound to ensure the secrecy and security of classified material.

Place

Date

Signature of the person bound by the obligation

Signature of the person imposing the obligation
Record of Clearance ☐ Approval for an activity and its restriction ☐ in accordance with section 10(4) of the CM Instructions

The relevant box is marked with a cross X

Mr/Mrs/Ms First name and surname
Date of birth

☐ was cleared today for access to CM at the following level
☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET

☐ received approval today for an activity in accordance with section 10(4) of the CM Instructions with the possibility of access to CM up to the following level
☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET

and was notified of his/her security obligations and the approach and recruitment methods of foreign intelligence services, as well as possible criminal-law and disciplinary-law penalties or labour-law implications in the case of any infringements (including dismissal).

☐ Clearance ☐ Approval is granted

☐ in general ☐ only for

☐ indefinitely ☐ for a period limited to

The following CM rules were handed over:

Place, date

Signature of the official Signature of the departmental head or security officer
Form 2  
(re section 11 of the CM Instructions)  
(verso)  

☐ Clearance  ☐ Approval was restricted today  

to classified material at the following level  

☐ CONFIDENTIAL  ☐ SECRET  

He/she declared that he/she had handed over all classified material at the following level  

☐ TOP SECRET  ☐ SECRET  

to the CM registry or successor, including all personal records and notes as well as any classified intermediate material  

Place, date  

Signature of the official  

Signature of the departmental head or security officer  

N.B.:  

A new form should be used if the clearance/assignment is extended to a higher classification level.
### Record of repeat notification

Mr/Mrs/Ms  
First name and surname  
Date of birth  
was again notified of his/her security obligations and the approach and recruitment methods of foreign intelligence services, as well as possible criminal-law and disciplinary-law penalties or labour-law implications in the case of any infringements (including dismissal).

<table>
<thead>
<tr>
<th>Place, date</th>
<th>Signature of the official</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

N.B.:  
The record of the repeat notification may also be included in lists or in form 2. The lists are to be kept for at least 5 years (as from the last entry).
Form 4  
(re section 12 of the CM Instructions)

<table>
<thead>
<tr>
<th>Record of</th>
<th>withdrawal</th>
<th>expiry</th>
<th>of the</th>
<th>clearance</th>
<th>approval</th>
</tr>
</thead>
</table>

Notification and delivery of the CM

The clearance for access to CM approval for an activity in accordance with section 10(4) of the CM instructions granted to Mr/Mrs/Ms First name and surname on has been withdrawn expired with effect from

His/her attention was drawn to the continuation of his/her security obligations, in particular of the obligation to keep the findings obtained from classified information secret.

He/she declared that he/she had handed over all CM to the CM registry or successor, including any personal records and notes as well as any intermediate material.

Place, date

Signature of the official Signature of the departmental head or security officer

N.B.
This record may be waived where clearance/approval is for a limited period.
### Form 5
(re section 18 of the CM Instructions)

<table>
<thead>
<tr>
<th>CM accompanying note</th>
<th>Number</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recipient (address)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level of classification</td>
<td>CONFIDENTIAL</td>
<td>SECRET</td>
</tr>
<tr>
<td>Reference number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The consignment contains the letter of</td>
<td>with</td>
<td>Annexes</td>
</tr>
<tr>
<td>The consignment is stored at</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Place, date</td>
<td></td>
<td>Signature of the official</td>
</tr>
<tr>
<td>To the CM registry</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Form 6  
(re section 18 of the CM Instructions)

<table>
<thead>
<tr>
<th>Department</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Place</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CM transfer record**

Today the field of activity of

**Name, title**

was transferred to

**Name, title**

The CM registers and CM receipt books as well as the keys to the CM safekeeping facilities, alarm and CM key safes were all available.

The whereabouts of the CM and its annexes were followed up and determined on a spot-check basis with reference to the following entries in the CM register:

<table>
<thead>
<tr>
<th>Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature of the person transferring the CM or witness (name, title)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature of the recipient (name, title)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Seen (signature of the departmental head or security officer)</th>
</tr>
</thead>
</table>
Form 7
(re section 18 of the CM Instructions)

Every destruction of one or more items of classified material is to be recorded as a separate destruction operation which can be continued on the reverse side or on additional pages. Obliques are to be entered in empty columns in such a way that subsequent entries are discernible.

<table>
<thead>
<tr>
<th>Serial number</th>
<th>Issuer</th>
<th>Reference number of the issuing body</th>
<th>Date</th>
<th>Reference number of own department</th>
<th>Primary copy number</th>
<th>With annex(es)</th>
<th>Only annexes (without cover note)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Destroyed on the orders of

_____________________________ on

Signature of the competent CM administrator (name, title) | Signature of witness (name, title)
<table>
<thead>
<tr>
<th>Recipient</th>
<th>CM receipt form</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number</td>
</tr>
<tr>
<td></td>
<td>sent on</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cover note</th>
<th>Annex(es)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference number (File number and CM register or log number)</td>
<td>Date</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

PROMPT return (non-classified) to

Department

Received on

Stamp and signature
Form 8d Form for CM exchange  
(re section 23 of the CM Instructions)

<table>
<thead>
<tr>
<th>Recipient (address)</th>
</tr>
</thead>
</table>

**CM receipt form**

<table>
<thead>
<tr>
<th>Number</th>
<th>Year</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>sent on</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Cover note**

<table>
<thead>
<tr>
<th>Reference number</th>
<th>Date</th>
<th>Primary copy no.</th>
<th>Number</th>
<th>Primary copy no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(File number and CM register or log number)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Annex(es)**

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Assurance of confidentiality:**
This is to assure that the classified material received is protected and handled in accordance with national regulations. Only appropriately cleared persons may have access to classified material at CONFIDENTIAL, SECRET and TOP SECRET level.

**PROMPT**

return (non-classified) to sender/courier

<table>
<thead>
<tr>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
</tr>
</tbody>
</table>

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Recipient

<table>
<thead>
<tr>
<th>Received on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
</tr>
</tbody>
</table>

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Stamp and signature
Form 8e Form for CM exchange  
(re section 23 of the CM Instructions)

<table>
<thead>
<tr>
<th>Recipient (address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM receipt form</td>
</tr>
<tr>
<td>Number</td>
</tr>
<tr>
<td>sent on</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cover note</th>
<th>Annex(es)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference number (File number and CM register or log number)</td>
<td>Date</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Assurance of confidentiality:**
This is to assure that the classified material received is protected and handled in accordance with national regulations. Only appropriately cleared persons may have access to classified material at CONFIDENTIAL, SECRET and TOP SECRET level.

<table>
<thead>
<tr>
<th>PROMPT</th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>return (non-classified) to sender/courrier</td>
<td>Received on</td>
</tr>
<tr>
<td>Department</td>
<td>Department</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

----------
Stamp and signature
Form 9  
(re section 25 of the CM Instructions)

<table>
<thead>
<tr>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Place</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Conference certificate

<table>
<thead>
<tr>
<th>valid until</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

It is hereby certified that, following a security check,

<table>
<thead>
<tr>
<th>Name, first name, title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date of birth</th>
<th>Place of birth</th>
<th>Nationality</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service/identity card</th>
<th>issued by</th>
<th>on</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

is cleared for access to classified material up to and including

<table>
<thead>
<tr>
<th>classification level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

On completion of the assignment for which it was issued, the certificate is to be returned to the issuing authority.

Signature of the departmental head or security officer

<table>
<thead>
<tr>
<th>Stamp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
Form 10
(re section 18 of the CM Instructions)

Authority

CM register

<table>
<thead>
<tr>
<th>Number</th>
</tr>
</thead>
</table>

for

Classification level(*)

This CM register comprises Number Double pages.

The rules in the CM Instructions are to be taken into account in keeping the CM register.

Signature of the security officer

Stamp

______________________________

Started
on

Kept
from – to by (name) Signature

______________________________

Concluded
on

(*) Enter applicable level of classification (TOP SECRET, SECRET, CONFIDENTIAL) using a stamp
### Form 10

**Left-hand double page**

- Page 1 -

**Continuation of Primary copies Annexes for SECRET**

<table>
<thead>
<tr>
<th>Serial number</th>
<th>Date</th>
<th>Letter</th>
<th>Receipt Dispatch</th>
<th>CM register number of the sender</th>
<th>CM level</th>
<th>Sender</th>
<th>Number of Primary copy no.</th>
<th>Number of pages</th>
<th>Number</th>
<th>Primary copy no.</th>
<th>Number of pages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject:</td>
<td>Type of operation</td>
<td>Submitted</td>
<td>File number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>-----------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Form 11

(Cover sheet)

Department

<table>
<thead>
<tr>
<th>CM receipt book</th>
<th>Number</th>
</tr>
</thead>
</table>

kept by

<table>
<thead>
<tr>
<th>Name, title</th>
<th>from</th>
<th>to</th>
</tr>
</thead>
</table>

kept by

<table>
<thead>
<tr>
<th>Name, title</th>
<th>from</th>
<th>to</th>
</tr>
</thead>
</table>

kept by

<table>
<thead>
<tr>
<th>Name, title</th>
<th>from</th>
<th>to</th>
</tr>
</thead>
</table>

This book has 25 double pages.

**Note**

CM receipt books help to keep records within the meaning of the CM Instructions. Entries should be made in ink or permanent biro. Any alterations must be discernible. They should be certified with the date and a signature. Any deletions must leave the original text legible. In CM receipt books there must be no erasures, rendering entries indecipherable or removal or addition of pages. CM receipt books should be kept in a safe place.
(*) If a whole file is being forwarded, it is sufficient to state the file number and the volume number (e.g. IS 4 - 607 023 Vol. 1). For individual CM items the number in the CM register (e.g. IS 2 - 32/94) may suffice.

<table>
<thead>
<tr>
<th>Serial number</th>
<th>Date</th>
<th>Reference number (*)</th>
<th>Primary copy no.</th>
<th>Annex(es)</th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

- 1 -
<table>
<thead>
<tr>
<th>Carrier</th>
<th>No. of the CM transport container</th>
<th>a) Time with sender</th>
<th>b) Meter reading with recipient</th>
<th>Confirmation of receipt (Name in block capitals, date, initials)</th>
<th>Return check</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td></td>
<td>a)</td>
<td>b)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>a)</td>
<td>b)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>a)</td>
<td>b)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>a)</td>
<td>b)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>a)</td>
<td>b)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-1a-

SN 3196/06

kin/GBK/cb/fc 21
Annex 4 to the CM Instructions

Guidance for the Marking of non-German CM

Non-German classified material (CM) should be marked as follows:

1. Non-German CM which the Federal Republic of Germany is under a treaty obligation to protect should be marked with the German classification that corresponds to the non-German classification assigned. Section 12(1) of the CM Instructions should be applied. It is sufficient to mark such CM with the German classification on the first page (Annexes or parts separately).

2. In the case of translations, where the non-German origin is not evident, this should be made clear on the first page next to the German classifications.

   Examples:
   (a) SECRET DEFENSE
       GEHEIM
       amtlich geheimgehalten
   (b) COSMIC TOP SECRET
       STRENG GEHEIM
       amtlich geheimgehalten

3. Below is a comparative list of the classifications used by organisations and States to which there are treaty obligations as indicated in point 1. In addition, with other States there are partial agreements for certain areas of cooperation which are known to the competent authorities (departmental agreements, project agreements). In cases of doubt, information is provided by the Federal Ministry of the Interior, which keeps track of all security agreements.

<table>
<thead>
<tr>
<th>Classification corresponding to those used by Germany</th>
<th>VS-NUR FRU DEN</th>
<th>VS- GEHEIM</th>
<th>STRENG GEHEIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIENSTGebrauch</td>
<td></td>
<td>VERTRAULICH</td>
<td></td>
</tr>
</tbody>
</table>

A. In international organisations:

1. NATO (1)  
   | NATO RESTRICTED | NATO CONFIDENTIAL | NATO SECRET | COSMIC TOP SECRET |
2. WEU (1)  
   | WEU RESTRICTED  | WEU CONFIDENTIAL  | WEU SECRET  | FOCAL TOP SECRET  |
3. EURATOM (2)  
   | EURA NUR FUR DEN | EURA VERTRAULICH | EURA GEHEIM | EURA STRENG GEHEIM |
   | DIENSTGebrauch  |                |            |              |
4. EUROCONTROL (1)  
   | EUROCONTROL     | EUROCONTROL     | EUROCONTROL | -              |
   | RESTRICTED      | CONFIDENTIAL    | SECRET      |              |
5. EUROPOL  
   | EUROPOL RESTRICTED | EUROPOL CONFIDENTIAL | EUROPOL SECRET | EUROPOL TOP SECRET |
6. EU  
   | RESTREINT UE    | CONFIDENTIEL UE | SECRET UE   | TRES SECRET UE/ |
   |                |                |            | EU TOP SECRET  |
B. In foreign States:

1. Belgium (5)
   - Diffusion: CONFIDENTIEL
   - Secret: TRÈS SECRET
   - Restricted: RESTREINT

2. Bulgaria (5)
   --Za Slušebno: SEKRETNOST
   - Polievank: SEKRETNOST

3. Denmark (5)
   - Til Tjenestenbrug: FORTROLIGT
   - Hemmeligt: YDERST

4. Estonia (5)
   - Asetkondukli: KONFIDENTSIAALNE
   - Salajane: APPORITON

5. Finland (5)
   - Käyttö: RAJOITETTU
   - Luottakulutelut: SALAINE
   - Erittäin: SALAINEN

6. France (5)
   - Confidential: DEFENSE
   - Très Secret: DEFENSE

7. Greece (5)
   - Periorismenos: EMPISTEITIKON
   - Apporiton: AKTROS

8. United Kingdom (5)
   - Restricted: CONFIDENTIAL
   - Secret: TOP SECRET

9. Italy (5)
   - Riservato: RISERVATISSIMO
   - Segreto: SEGRETISSIMO

10. Kazakhstan
    - Для Служебного: СЕКРЕТНО
    - Пользования: СЕКРЕТНО

11. Latvia (5)
    - Konfidenciali: SLEPENI
    - Slepens: SLEPENI

12. Lithuania (5)
    - Riboto: AUDOMO
    - Naudojimo: KONFIDENTIJA
    - Slaaptai: VISIKA

13. Netherlands (5)
    - Departementaal: CONFIDENTIEEL
    - Stoff: GEHEIM

14. Norway (5)
    - Begrensset: KONFIDENSIELT
    - Hemmelig: STRENGT

15. Portugal (5)
    - Reservado: CONFIDENCIAL
    - Secreto: MUITO

16. Rumania (5)
    - Secret de Serviciu: SECRET
    - Strict Secret: SECRETO

17. Russia
    - Для Служебного: СЕКРЕТНО
    - Пользования: СЕКРЕТНО

18. Switzerland (4/5)
    - Vertraulich: GEHEIM

19. Sweden-civil (3/5)
    - Hemlig: KVALIFICERAT
    - Military (3/5): HEMLIG

20. Slovak Republic (5)
    - Tajne: PRISNE

21. Switzerland (4/5)
    - Vertraulich: GEHEIM
Notes

(1) CM of these organisations is governed by rules which partly go beyond the requirements of the CM Instructions (e.g. in the case of NATO information that is COSMIC TOP SECRET and ATOMAL). The rules can be requested from the Federal Ministry of the Interior when required.

(2) The United States and France have no classification corresponding to "VS-NUR FÜR DEN DIENSTGEBRAUCH" ("RESTRICTED"). They manage and protect such CM of other States and international organisations under equivalent or stricter national rules;

(3) Sweden's civil authorities do not use any classifications comparable to "VS-NUR FÜR DEN DIENSTGEBRAUCH" ("RESTRICTED") or "VS-VERTRAULICH" ("CONFIDENTIAL"). German civil material classified as "VS-NUR FÜR DEN DIENSTGEBRAUCH" or "VS-VERTRAULICH" is protected in Sweden under the civil classification of "HEMLIG" ("SECRET") and keeps its German marking. Keeping the German marking ensures that e.g. any CM classified as "VS-NUR FÜR DEN DIENSTGEBRAUCH" which is protected in Sweden as "HEMLIG" and returned to Germany does not lose its original classification, unless technical reasons for so doing are indicated by Sweden.

(4) Switzerland does not use the classification "VS-NUR FÜR DEN DIENSTGEBRAUCH" ("RESTRICTED"). German CM with this classification is managed and protected in Switzerland in accordance with German security rules.

(5) In the case of States which are Members of the EU, NATO or the ESA, there may in the meantime have been changes in classifications which are not taken into account in the bilateral security agreements. Information on this can be obtained upon request from the Federal Ministry of the Interior.
Annex 5 to the CM Instructions

Guidance for CM Documentation

1. The CM rules, including circulars, notices and authorities' internal CM service instructions, must be easily accessible at any time to staff of the department.

2. In departments working with CM, a security policy tailored to the department should be drawn up, documenting the information and planned measures in line with the following points of the present Annex and in particular other provisions pursuant to section 4(3), section 18(1) and section 25 of the CM Instructions. In departments where material that is CONFIDENTIAL or classified at a higher level is rare, the security plan or parts thereof may be contained in other service rules or policies or refer to them (e.g. IT security policy).

3. List of the persons cleared or approved for access to CM pursuant to section 10 of the CM Instructions.

4. CM security documentation

   4.1. List of the locations, number and users of CM file security rooms, CM safekeeping facilities, CM transport containers, CM key safes and CM destruction equipment, of the places where the corresponding reserve keys and combination numbers are kept, and of the names of administrators and access facilities for emergencies,

   4.2. Documentation of guarding and technical surveillance; areas where alarm systems have been installed together with the arrangements concerning who may arm or disarm and service or repair them,

   4.3. Layout plans and admission arrangements for security areas and rooms equipped with anti-bugging devices,

   4.4. Records of checks carried out to ascertain whether

       4.4.1. the number of clearances for access to CM and approvals for work subject to security restrictions is necessary,

       4.4.2. persons cleared for access to CM and persons approved for work subject to security restrictions have been sufficiently vetted and informed of the security provisions to which they are subject,

       4.4.3. CM is produced, reproduced, marked, recorded, stored and circulated in accordance with the CM Instructions, and CM that is no longer required is discarded from the department's holdings pursuant to section 26 of the CM Instructions,

       4.4.4. the "need-to-know" principle is observed in practice.

5. IT-specific documentation

   5.1. Drawing up of a security policy in compliance with the procedure described in BSI Standards 100-2 and 100-3,

   5.2. Survey of the hardware and software, data carriers and other information technology used for CM together with the IT security functions employed,

   5.3. Documentation of usage and access rights,

   5.4. Documentation of acceptance and authorisation,

   5.5. Records of checks carried out to ascertain whether
5.5.1. IT security components are installed, serviced and repaired as prescribed,

5.5.2. access rights in the form granted are necessary, are correctly assigned in the IT system and the means of identification and authentication are protected in accordance with the rules,

5.5.3. unauthorised access attempts of any kind are followed up and repulsed, and

5.5.4. there have been cases of access to CM data that are clearly unjustified.

6. Reports on security incidents and documentation of cases which undermine security, together with measures taken and their results.
Annex 6 to the CM Instructions

Guidance for the Transfer and Dispatch of CM

N.B.: The following guidance applies chiefly to documents. For other forms of CM comparable protective measures should be taken.

1. Circulation of CM within the same building or a self-contained group of buildings

1.1. Within the same building, or a self-contained group of buildings, material classified as CONFIDENTIAL or above must be circulated from person to person or sent by messenger; the material must be recorded in a CM receipt book. It is not necessary to sign for receipt of material classified as CONFIDENTIAL or above which is circulated within a given department or organisational unit, or which is returned to the CM registry each day.

1.2. For material classified as SECRET, security officers may, exceptionally, waive the requirement to sign for receipt within a given department or organisational unit if there are special circumstances (an unusually large quantity of this kind of CM and unreasonable delays), provided that the whereabouts of the CM can be determined at all times. Material classified as CONFIDENTIAL may, if there is a particularly large quantity of this CM and if permission is given by departmental management, also be circulated to other organisational units without a receipt; the CM registry should be involved when CM is circulated. The whereabouts of such CM must be monitored closely.

1.3. Within a given site, material classified as SECRET or CONFIDENTIAL may be circulated from person to person or sent by messenger.

1.4. Material classified as RESTRICTED may be circulated without a receipt and sent on the same basis as unclassified documents.

2. Circulation of CM by messenger

2.1. When sent by CM messenger, material classified as TOP SECRET or SECRET must be sealed in self-adhesive folders or envelopes. The following wording must be placed on the adhesive strip or the envelope, together with the sender's signature:

"TOP SECRET/SECRET – this folder (this envelope) may only be opened by .................................. or the latter's representative holding TOP SECRET/SECRET clearance."

The self-adhesive folders or envelopes must be carried in sealed CM transport containers with a counter; in each case, the folders/envelopes must only contain CM for a single recipient. If CM transport containers with a counter are not available, a second envelope must be used as an outer cover, indicating only the recipient's address and the reference number, but not the classification level.

2.2. The sender must make the requisite entries in the CM receipt book. The CM receipt book must be given to the CM messenger. The sender must ensure that the receipt book is returned promptly and check the entries for completeness, to determine the time taken to circulate the CM and, if applicable, to verify that the counter readings tally.

2.3. The messenger must circulate the CM immediately and keep them in his possession until they are delivered. If material classified as TOP SECRET cannot be delivered immediately, it must be returned to the sender or to the relevant CM registry for temporary safekeeping.

2.4. The recipient must check that the CM transport container or envelope is undamaged and sealed, and open it personally. He must check the time taken to circulate the CM, and the counter reading if a CM transport
container is used, on the basis of the entries in the CM receipt book. He must enter the date and time, and the counter reading if a CM transport container is used, in the receipt book and sign for the CM.

2.5. When sent by messenger, material classified as CONFIDENTIAL must be sealed in self-adhesive folders, envelopes or other suitable packaging. The following wording must be placed on the adhesive strip or the envelope, together with the sender's signature:

"CONFIDENTIAL – this folder (this envelope) may only be opened by ………………………….. or the latter's representative holding CONFIDENTIAL clearance."

CM transport containers need not be used.
If the material is not signed for when circulated, the date and time of dispatch must be entered on the adhesive strip. Otherwise, Section 23(2) to (4) of the CM Instructions apply by analogy.

2.6. Consignments of material classified as CONFIDENTIAL or above which are marked "Personal" or "Not to be opened by the registry" on the inner envelope must be delivered unopened, with a CM accompanying note, to the recipient or the latter's representative. The recipient may determine that such CM should not be circulated in the course of events, if the "need-to-know" principle so requires. In this case only the completed CM accompanying note and the signed CM receipt form will be sent to the relevant CM registry.

3. Dispatch of CM

When material classified as CONFIDENTIAL or above is circulated between buildings on different sites, which do not form part of a self-contained group of buildings (dispatch), the following rules must be applied.

3.1. Material classified as TOP SECRET must be sent by CM courier.

3.2. CM couriers carrying material classified as TOP SECRET or SECRET must use an official car with driver. If this is not possible, a second CM courier must be used for material classified as TOP SECRET. The use of public transport, apart from taxis, must be avoided as far as possible, and avoided in all cases where material classified as TOP SECRET is concerned.

3.3. Material sent by CM courier must be placed in a neutral, locked CM transport container which has a lock fitted with a counter and a concealed label bearing the name of the department.

3.4. CM couriers must keep the CM in their possession at all times. If it is not possible to keep the CM being transported in their possession at all times, it must be stored as specified in Section 17 of the CM Instructions. If this cannot be done, it must be handed in, locked, to a police station for safekeeping.

3.5. Material classified as SECRET or CONFIDENTIAL may be carried by CM courier or private-sector delivery services. If a private-sector delivery service is used, the following conditions must be met:

1) Sender:
(a) clear address and reliable packaging,
(b) dispatch at latest possible time for delivery by midday on the next working day.

2) Private-sector delivery service:
(a) collection from sender with guarantee of delivery by midday on the next working day,
(b) proof of acceptance and delivery of the consignment,
(c) computerised tracking of consignments at every stage from acceptance to delivery.

If required, the BSI will advise which private-sector delivery services fulfil the criteria set out in point 2.
3.6. Material classified as RESTRICTED may be sent as an ordinary delivery.

4. **Dispatch or circulation of CM to parliaments, private individuals or companies**

4.1. CM which is to be made available to the Bundestag, or to the parliament of one of the Länder, should normally be sent by the highest Federal authorities to the CM registry in the administration of the Bundestag or of the Land Parliament for registration.

4.2. Before CM is circulated to private individuals or companies, a re-assessment should be carried out to establish whether all its elements need to be classified. If possible, the material should be classified at different levels, where this is appropriate.

4.3. For material classified as RESTRICTED, it is sufficient to incorporate the "Guidance for the Handling of Material Classified as RESTRICTED" (Annex 7) in the contract, or to draw these provisions to the attention of a private individual. Before circulating material classified as RESTRICTED to a company, an assessment should be carried out to establish whether it is essential to maintain the classification.

4.4. Section 22(4) of the CM Instructions applies to the circulation to companies of material classified as CONFIDENTIAL or above.

4.5. Private individuals may only be given access to CM when this is necessary in the interests of the State (for instance, in order to carry out an activity on behalf of the State). If the material is classified as CONFIDENTIAL or above, the individuals concerned must first be screened in accordance with the Security Screening Act and the general administrative regulations concerning security screening (see Section 35 of the Security Screening Act), made aware of the relevant provisions of the CM Instructions, required to give a formal undertaking to maintain confidentiality and informed that breach of confidentiality is a criminal offence and given clearance (Form 9). If necessary, the above provisions may be replaced by specific security regulations. CM may not be circulated to private individuals until measures have been taken to protect the CM, taking the CM Instructions into account as appropriate (for instance: temporary provision of a CM safekeeping facility).

5. **Dispatch of CM to recipients abroad**

5.1. Material classified as CONFIDENTIAL or above intended for legitimate recipients abroad should be sent via the Ministry of Foreign Affairs courier service to the relevant permanent representation of the Federal Republic of Germany; if the latter itself is not the recipient, it should be asked to forward the materials securely to the recipient, complying with the Ministry of Foreign Affairs' rules of procedure for the use of couriers (RES 21-23, section 1.16.3). If deliveries of CM subject to a deadline are not intended directly for the diplomatic representation but are made on behalf of other authorities, the requesting service must bear the costs incurred.

Material classified as TOP SECRET must also be encrypted or sent by double courier. Encryption for the civilian sphere is carried out by the Ministry of Foreign Affairs. The service sending the material must therefore contact the Ministry of Foreign Affairs.

5.2. Material classified as RESTRICTED sent from and to German diplomatic representations must also be sent via the Ministry of Foreign Affairs courier service. CM sent to other recipients abroad may be sent by a private-sector delivery service.

6. **Packaging of material sent abroad**

6.1. Material classified as CONFIDENTIAL or above must be sent in a double envelope. Except for material classified as CONFIDENTIAL, the envelope must not contain more than one item.

6.2. Inner envelopes must be of a type which has been certified by the Federal Office for Information Security as preventing any access to the contents.

6.3. The inner envelope must be sent marked with the following:
1) recipient and sender
2) name of the authorised recipient followed by "or representative",
3) classification level and
4) reference number.

6.4. If the contents of a consignment are intended, for a particular reason, only for the recipient named on the envelope, the inner envelope must be marked 'Personal'.

6.5. The outer envelope must only be marked with the details required for delivery. There must be no indications of the contents or that the consignment is subject to special treatment.

6.6. As an exception to the provisions of paragraph 1, consignments sent by courier should be packed in a single envelope marked with the reference number including the abbreviated classification level or an issue number. The courier and recipient must sign to confirm delivery.

6.7. When material classified as CONFIDENTIAL or above is sent by a private-sector delivery service, a completed CM receipt form must be enclosed in the inner envelope and returned by the recipient. If the CM receipt form is not received within a reasonable time (normally one week), the sender must issue a reminder requesting its return.

6.8. The above provisions apply by analogy to the dispatch of parcels.

7. **Storage of CM transport containers**

CM transport containers must be stored so as to prevent unauthorised access. The CM administrator must ensure that CM transport containers are returned to the CM registry immediately after use.
Annex 7 to the CM Instructions

Guidance for the handling of Material Classified as RESTRICTED

The purpose of this note is to lay down instructions for staff concerning the handling of material classified as RESTRICTED, and in particular for contracts with private-sector companies and organisations relating to the provision of goods or services classified as RESTRICTED. The specifications contained in this note should be included in the provisions of such contracts.

I. General

1. Access authorisation and circulation

1.1. Material classified as RESTRICTED may only be made available to persons who need to have access to it in order to carry out their duties, or prepare for them ("need-to-know" principle). Those granted access must, demonstrably, be familiarised with this note before being given access to CM of this kind, and made aware of their particular responsibility to protect CM, as specified in this note, and of the consequences – in terms of criminal prosecution, or legal action for breach of contract – should they fail to do so.

Additional measures, such as security procedures by the Federal Ministry of Economics and Technology, security assessments or formal notification of visits, are not necessary at this level of security classification.

1.2. The contents of the CM must not be circulated to non-participating third parties. Staff who have proven to be unsuited to handling such CM or who have violated confidentiality obligations must not be permitted to handle such CM.

1.3. Material classified as RESTRICTED may only be circulated to government agencies, international organisations or contractors which are participating in a programme/project/contract and need to access the information in order to implement the programme/project/contract. Written permission must be obtained from the CM contract awarding body before circulating material classified as RESTRICTED to non-participating international organisations or contractors from non-participating countries. This will normally require a confidentiality agreement (see Section 23 of the CM Instructions).

1.4. In Germany, the Federal Ministry of Economics and Technology can ensure that the CM contractor is complying with the provisions of this note. If the contract awarding body is a government authority, it can also exercise this supervisory function itself in accordance with the first sentence.

1.5. The CM classification expires thirty years after 1 January of the year following classification, unless a different time-period is specified. In the case of international contracts, the Federal Ministry of Economics and Technology must be consulted if there are no programme or project agreements (see Section 26 of the CM Instructions).

2. Handling procedures

2.1. Marking, handling and storage

Documents and equipment classified as RESTRICTED must be marked, handled and stored as follows:

2.1.1. Documents – including all similarly classified Annexes – must be marked "CLASSIFIED MATERIAL – RESTRICTED", with a stamp in black or blue ink, at the top of each page (excepting blank pages). International or foreign CM must be restamped with the appropriate German marking. Books, brochures etc. need only be stamped on the cover and title page. If the foreign classification is marked on each non-blank page of a foreign book or brochure, it is sufficient to stamp the German classification on the cover or title page.
2.1.2. Equipment or data carriers (e.g. diskettes, CDs, microchips, microfiche) classified as RESTRICTED must also be marked or re-stamped, either in a clearly visible way on the equipment or data carrier itself or – if this is not possible – on its storage container.

2.1.3. CM must be stored in locked rooms or containers (cupboards, desks etc.). If removed from such rooms or containers, it must at all times be stored and handled in such a way as to prevent unauthorised persons gaining access to or being able to inspect the CM.

2.1.4. Intermediate CM (e.g. preliminary drafts, shorthand transcriptions, sound storage media, transparencies) must be protected against inspection by unauthorised persons in the same way as the document to which it relates. Intermediate CM which is not passed on to third parties and is immediately destroyed need not be marked as CM.

2.2. Circulation

2.2.1. Within Germany, CM is circulated by messenger or dispatched by delivery service in a single sealed envelope or container. The envelope or container is not marked "CM".

2.2.2. CM can be sent abroad by private delivery services as an ordinary letter or parcel, or as air or sea freight, unless the CM contract awarding body has explicitly opposed this means of dispatch or specified other arrangements for its dispatch abroad. When doing so, the CM contract awarding body must comply with international agreements and/or specific programme or project agreements.

2.3. Destruction/return

2.3.1. To avoid the accumulation of large quantities of CM, CM which is no longer required must be destroyed or returned to the CM contract awarding body.

2.3.2. CM and intermediate CM must be destroyed in such a way that the contents can no longer be identified or recovered.

2.4. Loss, unauthorised circulation, finding of mislaid CM or non-compliance with this note

In the event of loss or unauthorised circulation of CM, of mislaid CM being found or of non-compliance with this note, the German CM contract awarding body and the Federal Ministry of Economics and Technology (Dept VI B 3) must immediately be notified via the private organisation's security officer – if appointed – so that potential damage can be limited and the incident investigated.

2.5. Visits

Visits to or from foreign countries involving access to material classified as RESTRICTED, or at an equivalent classification level, are normally agreed directly by the sending institution and the host institution. There are no specific formal requirements.

2.6. Contracts

2.6.1. The CM contract awarding body must impose a contractual obligation on all CM contractors/subcontractors to comply with the provisions laid down in this note and inform them that the contract, or parts thereof, may be revoked in the event of non-compliance.

2.6.2. In connection with tenders or invitations to tender, and after a contract has been performed, CM must be stored in accordance with the specifications until it has been de-classified, and destroyed or returned as soon as possible.

2.6.3. Foreign CM contractors/subcontractors must be contractually obliged to comply with the specifications laid down by their security authority for the handling of CM of a comparable classification level. If no comparable classification level exists in the CM contractor's/subcontractor's country, the Federal Ministry of Economics and Technology (Dept VI B 3) should be consulted so that it can agree protection rules with the foreign security authority concerned. Permission must then be obtained from the Federal Ministry of Economics and Technology before the relevant CM is circulated.

II. Use of information technology (IT)

1. Processing

1.1. If IT is used to process material classified as RESTRICTED, IT measures and/or physical and organisational measures to protect the CM (as detailed in sections I 1.1 and 1.2) must be implemented.
1.2. Before processing or storing material classified as RESTRICTED, it must be ensured that the machine, or the internal network, is not connected directly (e.g. without firewall protection) to the Internet, unless additional measures as detailed in section 3.3 have been taken.

1.3. The following measures, in particular, apply when processing material classified as RESTRICTED:

- listing those authorised to access the CM,
- use of identification and authentication mechanisms (e.g. login, password),
- appropriate IT security instructions (for individual workstations or for the organisation as a whole).

Wireless keyboards and networks may only be used if they have been approved by the Federal Office for Information Security (BSI).

1.4. If portable IT systems (e.g. notebooks or handhelds) are used to process or store material classified as RESTRICTED, the storage media used must be encrypted with BSI-approved products. If BSI-approved programmes and devices are not available, products certified by the BSI to Common Criteria EAL 3 or above may be used.

1.5. Portable data carriers (e.g. diskettes, CDs, removable disk storage) containing unencrypted data classified as RESTRICTED must be marked as specified in section I 2.1.2 and stored as specified in section I 2.1.3.

1.6. Data carriers must be erased using software products which overwrite them at least twice. BSI-recommended products should be used.

1.7. IT equipment and data carriers must be checked for viruses (especially Trojans or worms) before being used to process material classified as RESTRICTED. These checks must be carried out at regular intervals.

1.8. Personal IT equipment (e.g. laptops), software or data carriers must not be used to process material classified as RESTRICTED. Personal software or data carriers may not be used in IT systems in which material classified as RESTRICTED is processed.

1.9. Material classified as RESTRICTED which is stored unencrypted on permanently-installed data carriers must be deleted as specified in 1.6 before the data carriers leave the possession of persons authorised to access CM for the purpose of maintenance or repair to IT system components. If deletion is impossible, the data carriers must be removed and retained, or the maintenance/repair firm must be contractually obliged to comply with the rules laid down in this note.

2. Transmission

2.1. When transmitted electronically via telecommunications or other technical communications links (including online services such as WWW, FTP, TELNET, e-mail etc.) in Germany, CM must be encrypted using an encryption system which is BSI-approved and certified (Section 40 CM Instructions) or approved by the Federal Ministry of Economics and Technology. Exceptionally, unencrypted transmission is permissible:

(a) within fixed networks, in the case of telephone conversations, videoconferences and fax or telex transmission, if there is no encryption facility available between sender and recipient for the form of transmission required and if the CM contract awarding body does not explicitly request encryption when awarding the contract. Before transmission, the sender must take all possible steps to ensure that it is connected to the right recipient,

(b) within a closed network (LAN), if it is operated solely on a single geographically continuous company-owned site and the transmission installation is protected against direct access by unauthorised persons.

2.2. In the case of international electronic transmission, encryption procedures must be agreed by the national security authorities of the participating States. If specific transmission security instructions are agreed for an individual programme/project, these must be complied with. The Federal Ministry of Economics and Technology (Dept VI B 3) will provide further information if required.

3. Measures to ensure confidentiality

The measures recommended below are intended to ensure the confidentiality of electronically stored CM. They are not intended primarily to ensure the integrity or availability of data.

A distinction needs to be drawn between three different situations:
3.1. **Standalone PCs or networks with closed user groups which are not connected to other networks**

- The operating system must provide for a differentiated user profile and access protection down to the level of individual files, to ensure that the "need to know" principle can be applied (e.g. Unix/Linux; Win NT; Win 2000, Win XP).
- There must be a login and password. The password must contain at least 6 alphanumeric characters, including special characters, capitals and lower-case letters.
- The BIOS must also be password-protected.
- It should normally be possible to boot the IT system only from the hard drive.
- If possible, the system should include a RAM disk for Temp files (help).
- An up-to-date virus protection programme must be used.
- In networks, a separate partition should be installed on the server for the storage of CM data.

3.2. **Closed networks with external e-mail connection**

In addition to the points listed in 3.1,

- there must be a server-based network with the server in an access-protected area,
- there must be a firewall, either on the server or as a separate IT system (and, if applicable, an additional e-mail server), also in an access-protected area,
- a packet filter must be used; an application gateway is a possibility,
- all IP addresses apart from the server IP must be hidden (DNS server),
- material classified as RESTRICTED must be transmitted encrypted. Only products approved by the Federal Ministry of Economics and Technology may be used for encryption. Keys should not normally be stored on the hard drive. Mandatory user rules must be laid down within the organisation and users must be trained to apply them. The latest security updates for the software used must be incorporated as they become available, especially in the firewall.

3.3. **Standalone PCs or closed networks with e-mail and Internet connection**

In addition to the points listed in 3.1 and 3.2,

- there must be a firewall and an application gateway,
- the password rules set out in the BSI Basic Protection Manual must be applied,
- data relating to material classified as RESTRICTED must be stored on the server in a separate partition or a specially protected data area; the protection mechanisms thus created must be utilised accordingly.

Depending on the size of e.g. a user group or project, it may be necessary to establish VPN protection specifically for it.
Annex 8 to the CM Instructions

Guidelines for the Transfer of Classified Material to the Secret Section of the Federal Archives
(CM Archiving Guidelines)

Section 1 General/Basic principles
1. Under the Act on the security and use of federal archive material (Federal Archives Act)\(^1\), Federal Government archive material must be permanently secured and made accessible. Without the permission of the competent archive department therefore, classified material cannot be destroyed.
2. Unduly long periods of storage of CM documents in secret registries can lead to partly irreparable conservation damage or even loss. Early transfer of CM no longer or not currently required for work purposes to the secret section of the Federal Archives, is therefore urged.

Section 2 Secret Section\(^2\)
1. The secret section of the Federal Archives stores material classified as TOP SECRET, SECRET and CONFIDENTIAL which is no longer or not currently required for administrative purposes.
2. Complete items of material to be stored (e.g. binders, standing files, films or tapes) should be transferred to the secret section. The file order is not to be changed (e.g. documents are not to be removed).
3. Addresses and further details are contained in the information sheet on "Discarding and transferring CM to the secret section of the Federal Archives". The information sheet and forms for listing the material transferred and for declassification of material are available on the Federal Archives' website – www.bundesarchiv.de.

Section 3 Determining conservation time and the duration of classification
1. Before transferring CM, the transferring office must determine the final year of the storage period and the classification for each item of stored material.
2. The storage period should be as short as possible and is to be set independently of the classification. Section 19 of the Registry Guidelines is to be applied as appropriate.
3. For German CM, the period for declassification is determined in accordance with Section 9(1) to (4) of the CM Instructions.
4. In the case of apparently unjustified classification periods, especially where excessively long, the Federal Archives have the right to apply to the highest competent federal authority for a review of the reasons for the classification.

---
\(^1\) Act on the security and use of federal archive material (Federal Archives Act – BarchG), 6 January 1988 (BGBl. I p. 62), as last amended by the Act Amending the Federal Archives Act, 5 June 2002 (BGBl. I p. 1782).
\(^2\) Federal Archive (intermediate section), Bundesgrenzschutzstr. 100, 53757 St. Augustin; and Federal Archives (military section), 79024 Freiburg.
Section 4 Processing of classified material in the Archives

1. The secret section records stored items in the transfer lists.
2. The secret section makes the classified material available again to the transferring authority at its request.
3. The secret section may process the classified material deposited with it for archive purposes, provided that it is not sealed or specially secured in any other way.
4. After declassification, documents suitable for archiving become part of the Federal Archives' holdings. CM not suitable for archiving is destroyed when the storage period has expired.
5. By derogation from Section 27(3) of the CM Instructions, destruction is recorded in the transfer list.

Section 5 Use of CM by third parties

1. The use of CM in the secret section of the Federal Archives by third parties requires the prior permission of the transferring authority. Permission is only to be given where the use is officially justified or is in the official interest and consistent with the need for security of the CM in question. Where the security interests of other authorities are concerned, the transferring authority must first reach agreement with them.
2. Before giving permission for use of CM by third parties (e.g. scientific use), the possibility of disclosure of the CM must be considered. CM which has been made available to third parties for their use should be disclosed in the interests of science, equal treatment and verifiability of the results of use.
3. The provisions of Section 5(5) of the Federal Archives Act and Section 39 of the Common Rules of Procedure apply as appropriate.

Section 6 Final conditions

1. Any change in responsibility for CM stored in the secret section as a result of reallocation of tasks must be notified in writing. Before onward transfer of CM documents to the office assuming responsibility under Section 23 of the Registry Guidelines, the office hitherto responsible must verify which classified material may be transferred to the secret section.
2. The Ministry of Foreign Affairs and the Federal Ministry of Defence may issue independent rules for their own fields which with the basic principles of these Guidelines.
Information Sheet
on the discarding of CM and its transfer to the secret section of the Federal Archives

I. General

1. The discarding of CM is governed by Section 26 in conjunction with Annex 8 (CM Archiving Guidelines) of the CM Instructions.
2. Correspondingly, for transfer of CM to the secret section, Section 20 of the Registry Guidelines applies. The cover page for the list of classified material transferred to the secret section and the list itself (transfer list) are attached here for downloading as Annexes 2 and 3.
3. For material classified as RESTRICTED and for documents from which the classification has been removed, the rules laid down for unclassified documents apply.
4. CM the storage period of which has expired and which will clearly not acquire lasting value may be destroyed on the spot with written permission from the Federal Archives (see Section 22 of the Registry Guidelines).
5. Where there are problems and queries relating to discarding, the heads of the secret sections in St Augustin and Freiburg will help, as will the archivists in Koblenz, Berlin or Freiburg.

II. Technical guidance for transfer

1. It is recommended that each file identified for discarding (each storage item) be submitted to the competent processor with a corresponding form. The following information should be given on the form:
   – whether and when this storage item is to be discarded
   – whether and until what year it should be kept available for retrieval (storage period)
   – in which year the material is to be declassified.
2. If the material is declassified at the time of transfer of the documents, this should be noted on the storage item (see Annex 1). Transfer is in accordance with the procedure for public documents.
3. CM documents should be supplied and where applicable deposited in the order followed in the CM Registry. A new or revised order is therefore to be avoided. There must also be no subsequent removal of individual documents from a file or collation in another document holder.
4. In the transfer list (Annex 3), the files should be listed fully and accurately. This applies in particular to file numbers and lists of contents, with contents being drawn up so that the transfer list is not classified at a level higher than RESTRICTED. Careful completion of the cover page (Annex 2) will facilitate later retrieval.
5. The transfer list with its cover page should be submitted to the Federal Archives in paper or electronic form. The secret section transmits to the transferring office a copy of the transfer list with the registered archive numbers.

6. For later archive processing of the CM transferred to the secret section, the Federal Archives should also be provided with the corresponding CM filing scheme (where one exists) and the CM file list; but not document-based CM storage lists (e.g. log).

III. Further guidance

1. As in the case of public documents, it is essential to group together similar subjects in readiness for processing in subject files (individual, collective and special subject files); attention is drawn to the corresponding rules in the Registry Guidelines and the comments in the "Recommendations for document management". With a view to facilitating later discarding, voluminous documentation from other offices can be filed separately where processing does not make grouping together advisable.

2. Authorities keeping files and the Federal Archives may agree that, in addition to intermediate CM and technical installations (e.g. technical models), certain sets of CM may be destroyed directly within the authority on its own responsibility. These sets should be included in a catalogue of material for discarding and evaluation. In doubtful cases (e.g. where there is the prospect of discarding voluminous documentation), the competent Federal Archives archivist may determine the documents to be transferred to the secret section in the CM Registry, as part of preliminary evaluation.

3. In the case of documentation taking the form of a fairly large number of documents of the same type (especially "case" files), the Federal Archives will be grateful to receive relevant comments from archive staff who are familiar with the content of the files and can make a specialist assessment. Files are considered for long-term conservation principally on the basis of the significance of the case or the content or because of particular features (e.g. new technical procedures). In doing so, archive staff should in some suitable manner (e.g. on the cover page) mark the storage items which in their view require long-term conservation. The marking may already be done at the time of filing or only when conservation times are assigned.

4. The provisions of Central Service Instruction 64/3 – RESTRICTED, "Processing and securing Federal Armed Forces documents in peacetime and in time of alert", should be observed when transferring CM from the sphere of the Federal Ministry of Defence.

IV Processing of CM in the secret section of the Federal Archives

1. When transferred documentation is being checked, verification by the secret section is restricted to storage items (files) and does not cover individual documents.

2. The Federal Archives may still in individual cases destroy the documents received in the course of archive processing – following expiry of any applicable storage periods.

3. The secret section notes any declassification of CM on the storage item (see Annex 1).
4. After declassification of CM and archive indexing, documents of archive value are moved to the corresponding public archive at the final archives in Koblenz. On request the relevant authority receives notice of the ultimate disposal of a CM storage item.

V. Further information

Rules for document management
The Federal Ministries' Common Rules of Procedure of 2000 and the Guidelines for Document Processing and Management (Files and Documents) in Federal Ministries of 2001 may be viewed on www.staat-modern.be. Paper versions may be ordered from bestellservice@bva.bund.de. The 2001 Guidelines can also be used as a model for non-ministerial departments. Details are contained in the information sheet on "Non-ministerial Federal Administration Departments and the Federal Archives" (www.bundesarchiv.de).

Recommended reading on document management in German

Information on the Federal Archives
- Information at the website www.bundesarchiv.de
- The Federal Archives, Servicing Research, the Public and Administration, Koblenz 2002, 137pp.

Addresses for the Federal Archives
Federal Republic of Germany Department
66064 Koblenz
Potsdamer Str. 1, 56075 Koblenz
Tel.: 0261/505 0
Fax: 0261/505 226
e-mail: koblenz@barch.bund.de

and
12175 Berlin, Postfach: 450 569
Finckensteinallee 63, 12205 Berlin
Tel.: 01888/777 0
Fax: 01888/777 111
e-mail: berlin@barch.bund.de

Secret Section
Bundesgrenzschutzstr. 100, 59757 St. Augustin-Hangelar
Tel.: 01888/74000 0
Fax: 01888/74000 33
e-mail: zwarchst.aug@barch.bund.de

Military Archives and Military Secret Section Department
79024 Freiburg
Wiesentalstr. 10, 79115 Freiburg
Tel.: 0761/47817 0
Fax: 0761/47817 900
e-mail: militaerarchiv@barch.bund.de
Department

Place

Date

Declassification

The following storage item

Subject

Reference number

is declassified with effect from .................................................................

........................................
(name, signature)           Stamp

3 If this form is used by the Federal Archives (see IV(3)), only the archive call number should be inserted here.
# Annex 2

**Cover page to list for transfer of CM to the secret section**

Notes for completion:
- Complete as fully as possible
- Complete reverse of page if necessary (giving line numbers)
- Lines 5 to 7 are only to be completed for files
- Please take account of footnotes

<table>
<thead>
<tr>
<th></th>
<th>To be completed by the secret section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Archive call number</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Transferring authority (short title)</td>
<td>Number of storage items</td>
</tr>
<tr>
<td>3</td>
<td>Unit giving permission</td>
<td>Date</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Extension</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Signature</td>
</tr>
<tr>
<td>4</td>
<td>Transfer from CM Register</td>
<td>Transfer on¹</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Extension</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Brief description of content according to information in the organisational or work allocation scheme, where possible for the final year of the files' period of validity²</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Period of validity (years of oldest and newest document)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Nomenclature of filing scheme sections with markings and definitions³</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Last organisational unit(s) keeping files⁴</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Further organisational units keeping files in the period in question⁵</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(a)</td>
</tr>
<tr>
<td></td>
<td>(b)</td>
</tr>
<tr>
<td></td>
<td>(c)</td>
</tr>
<tr>
<td></td>
<td>(d)</td>
</tr>
<tr>
<td></td>
<td>(e)</td>
</tr>
<tr>
<td></td>
<td>(f)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Remarks (e.g. state time-periods and reasons therefor in accordance with section 5(2) and section 7(2) of the CM Archiving Guidelines.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

¹ Serves also as date of issue of transfer list.
² For transfers regarding (sub-) divisions, it is only necessary to complete the subject description of the (sub-)division. If this is not possible, only field 7 should be completed.
³ For large transfers, often only a general description is possible (e.g. only stating the main groupings in the filing scheme).
⁴ Note 4 to Annex 3 should be followed in sequencing documents from several organisational units by file number.
⁵ All important organisational units keeping files should as far as possible be indicated for the period stated in field 6 (also those of precursor authorities, where applicable) together with the dates of the changes in responsibility or nomenclature. If the period of responsibility cannot be established, a date falling within the period should be given.
### List for the transfer of … to the secret section (transfer list)

<table>
<thead>
<tr>
<th>Serial number</th>
<th>Archive number</th>
<th>File number</th>
<th>Contents</th>
<th>Volume number</th>
<th>Period from</th>
<th>Period to</th>
<th>Classified until 31.12….(year)</th>
<th>Classification</th>
<th>To be stored until 31.12….(year)</th>
<th>For destruction (note)</th>
</tr>
</thead>
</table>

---

4. The details in the transfer list should be chosen so that no higher level than RESTRICTED is necessary.

5. Each storage item in accordance with section 3(3) (for files: according to type of filing, folder or binder) receives a serial number; the numbers should each be listed separately and should be repeated for each listed file of the same storage item.

6. This column is completed by the secret section. For any subsequent requests, only the archive numbers should be given.

7. For files only: subject order according to the file plan. In addition, the organisational unit keeping files may be indicated in a separate column where documents from several organisational units are shown according to the order in the file plan.

8. For files, the serial number of the volume should be given, not the number of volumes.

9. Only the following capital letters should be used: T (= Top secret), S (= Secret), C (= Confidential), R (= Restricted).

10. Date and signature of the person completing the form and witness.