Current status

**Released**

Document name

| Registration No. | Edition | Page | Enclosures |
|---|---|---|---|
| 2008-09643E | 14 | 1 (9) | 0 |

| Issuing date | Valid from | Valid until |
|---|---|---|
| 21 April, 2026 | | |

Title

# Quick guide - Information Security

| | |
|---|---|
| Issued by | Per Rehn/S |
| Linguistic check | Nej |
| Factual review | No |
| Quality review | No |
| Project approved | No |
| Line approved | Per Rehn/SG/2026-04-27 |
| External review | No |
| Released | Admin, OKG, 2026-04-27 |

Subject No.

Distribution
Publiceras via ledningssystemet

Classification level

**Public**

# Revision list

| Edition | Reason for revision/Sections concerned | Issuer (sign/dept) | Issued (dd.mm.yyyy) |
|---|---|---|---|
| 14 | Converted to M541E. Document name 1.3. Revised title Quick guide. Complete review. Changes are highlighted in the right-hand margin. | PRR/SG | 2026-04-21 |

**Table of Contents** **Page**

# 1 Affiliation of the Quick guide

## Affiliation to the process

-

## Affiliation to the assigned task

The Quick guide emanates from the task ”Informations- och IT-säkerhet, process och kommersiell IT” (*Information and IT security, process and commercial IT*) pursuant to 2005-08528 ”VDs organisation och uppgiftsfördelning” (*MD's organisation and task distribution*).

## Affiliation of the Quick guide to other documents

The Quick guide is based on instructions 2011-02371E ”Regulations for Information Security” and 2007-21444 ”Regulations for IT Security” regarding selected sections for handling information from a confidentiality standpoint. For the rules in their entirety, please refer to these documents.

# 2 Information Security

## 2.1 Classification of information

To ensure a high level of information security, information is classified. The classification specifies the requirements that apply to storage, distribution, destruction, etc.

***Authorised*** to access the information, are the individuals who need the information in order to be able to carry out their duties, who have been security cleared, who have signed a confidentiality agreement and who have adequate knowledge of information security/protective security.

## 2.2 Reclassification of information

Reclassification may be performed at the request of the issuer of the information.

## 2.3 Exchange of information with authorities

Swedish authorities apply the principle of public access to official records. When in contact with the authorities, request for maintained secrecy must be made for documents that are classified confidential, secret or top secret.

## 2.4 Exchange of information with other external parties

When exchanging classified information with an external party, a non-disclosure agreement must have been signed, and in some cases also other supplementary agreements.

OKG's internal regulations for classification, marking, storage, distribution and destruction shall be applied as a basis at the issuance of specific procedures for the handling of OKG information at external parties.

***USB flash drives*** - restrictive handling must be applied, please see instruction 2007-21444E *Regulations for IT Security*.

## 2.5 Marking

Documents are marked so that the recipient is given a clear indication that special handling regulations apply. Marking also has a legal function as it determines what section of a law is referred to for the purpose of protecting the contents against unauthorised distribution.

Information that is newly produced or revised/updated must, irrespective of classification level and with the exception of classification level public, always be marked by using templates in applications or stamps.

Documentation that lacks marking or that has another kind of marking than the type specified in 2011-02371E – *Regulations for Information Security*, must be marked with the valid marking in force before distribution outside of OKG may take place.

## 2.6 Description of classification levels and handling rules for these

Information must always be classified and marked when produced or received.

At OKG, the following classification levels are used:

- Public (Swedish "Öppen")
- Restricted (Swedish "Intern")
- Confidential (Swedish "Intern med begränsad spridning")
- Secret (Swedish "Hemlig", security classification level Restricted)
- Top Secret (Swedish "Kvalificerat hemlig", security classification level Confidential and Secret)

### 2.6.1 Public

Public information is of the type by which its dissemination is desirable and not restricted by any requirements on marking, storage, distribution or destruction.

### 2.6.2 Restricted

Restricted information is of the type by which its dissemination, unauthorised use of or change in content would lead to restricted or minor damage to the company or a person.

***Physical storage***
May be stored openly within OKG's premises but protected against unauthorised access. Outside OKG, this kind of information must be kept under observation or stored in a locked space.

***Electronic storage***
Information must be protected by the use of access control and an authorisation management system.

***Distribution***
May be distributed within OKG. External distribution is permitted ***provided that*** the recipient is authorised.

***Destruction***
At OKG, information is processed through the normal paper recycling system. Outside OKG, information must be destructed in order to prevent unauthorised dissemination.

***Electronic destruction***
Regarding storage media for which deletion is not possible, e.g. CD/DVD, physical destruction must be performed. Storage media should be handed over to the archives staff at GAI (E3 O3) for further destruction according to current procedures.

### 2.6.3 Confidential

The type of information which could be used as a source of information prior to sabotage, attack, act of terror or theft of nuclear material or nuclear waste, which also applies to information that may be covered by export control. This includes photos of technical installations and equipment at OKG. The standard procedure for technical documentation is its classification as confidential. There are exemptions for which also classification levels restricted or public may be used, please refer to 2011-02371E *Regulations for Information Security.* If stronger protection

is required, the documentation is classified as secret or top secret.

***Physical storage***

May be stored openly within OKG's premises but protected against unauthorised access. Outside OKG, the information must be stored in a secure manner within locked premises protected against unauthorised access.

***Electronic storage***

Information must be protected by the use of access control and an authorisation management system.

Regarding electronic storage outside OKG, it is required that OKG conducts a review of external companies' premises, IT environments and the like. The use of an external cloud services is ***not*** permitted.

***Physical distribution***

May be distributed within OKG. External distribution is permitted ***provided that*** the recipient is authorised. Information shall be sent as Registered Mail with the additional service Recipient confirmation/Proof of receipt, or be sent as Valuables with additional service Recipient confirmation. The item of mail must be wrapped and sealed in such a manner that unauthorised opening of the item cannot take place without causing visible damage to the wrapping or the seal. At OKG, external distribution including bookkeeping and making sure that the item reaches the recipient is handled by subsection Shared Services, Administration, Service.

***Electronic distribution***

External distribution must be encrypted. OKG provides two different solutions for how this may be done:

- encrypted files/e-mail (PGP, PKI, 7-Zip or AxCrypt)
- encrypted file server solution (secure FTP)

***Physical destruction***

At OKG, information is processed through the normal paper recycling system. Outside OKG information must be destructed in a document shredder with a so-called cross-cut function.

***Electronic destruction***

Electronic storage media (USB flash drive, CD/DVD etc.) should be handed over to the archives staff at GAI floor E3O3 for further destruction in accordance with applicable procedures.

### 2.6.4 Secret

Type of information which gives the company a clear advantage over its competitors and where the disclosure, dissemination, use or change of which could be damaging to the company or a person. Secret information ***also comprises information of security classification "restricted***", which may result in minor damage to the national security of Sweden in the event of disclosure.

**Physical storage**

When stored in a space within the OKG protected area, at an external OKG office or contracted and audited company, information must be kept in a safety cabinet classified with burglary class SS 3492, alternatively SSF 3492. When carried to or from the place of storage as described above, the information must be kept under control.

In areas where secret information is handled, measures shall be taken to obstruct unauthorised view or the possibility to look in at the premises by using curtains, blinds, privacy protection, closed door, etc.

***Electronic storage***
To be processed in a separate security network that has no connection with other IT systems. Access to the application must take place via two-factor authentication. Print-outs are permitted if performed on special printers that require personal identification before the print-out is initiated. OKG must also conduct a review of the network. Outside OKG, it is required that OKG conducts a review of the company's premises, IT environment and the like.

***Physical distribution***
Within the premises of OKG, distribution of information of this classification level must take place by delivery in person. External distribution is permitted ***provided that*** the recipient is authorised. The information shall be sent as Registered Mail with the additional service Recipient confirmation/Proof of receipt, or be sent as Valuables with additional service Recipient confirmation. The item of mail must be wrapped and sealed in such a manner that unauthorised opening of the item cannot take place without causing visible damage to the wrapping or the seal. At OKG, external distribution including bookkeeping and making sure that the item reaches the recipient is handled by subsection Shared Services, Administration, Service. Prior to distribution outside Sweden may take place the information manager must be contacted for an assessment whether or not the distribution is permitted in accordance with the legislation in force, and for a risk assessment of the chosen distribution method.

Distribution to a recipient that is not on the original distribution list must be approved by the issuer of the information (provided that the individual works within the same area of responsibility) or by the information officer responsible and be recorded by updating the distribution list.

If conversations classified as Secret are to take place at the premises, electronic equipment that has an eavesdropping or recording function (such as mobile phones, smartwatches, smart speakers and Bluetooth devices) must be left outside the room in which the conversation takes place.

***Electronic distribution***
Internal distribution at OKG is primarily performed via the application named Secret Oden. Distribution by the use of encrypted (PGP, PKI, 7-Zip) CD/DVD or USB flash drives approved by OKG may take place provided that the above-mentioned regulations for physical distribution are complied with. Information must not be discussed over the phone.

***Physical destruction***
To be destructed in a document shredder with a so called cross-cut function.

**Electronic destruction**
Storage media (USB flash drive, CD/DVD etc.) are handed over to archive staff at GAI floor E3O3 for further destruction in accordance with applicable procedures

### 2.6.5 Top secret

***Refers to information of security classification level Confidential and Secret*** which in the event of disclosure could result in a not insignificant damage to the national security of Sweden. Top secret information is stored at the Security Manager's office and handled according to separate procedures.

# 3 References

-