

Information Security – Manual

This manual describes how we at OKG, for reasons of secrecy, handle documents. In order to be able to achieve complete information, please see instructions 2005-10597E ” *Regulations for Information Management at OKG*” and 2007-21444E ” *Regulations for IT Security*”.

Secrecy classification

In order to be able to achieve a high level of information security, use is made of the term secrecy classification. Secrecy classification specifies the requirements that apply for storage, handling, distribution, etc.

OKG can require from other companies and authorities along with individuals that they shall protect our information, provided that it has been secrecy classified by us beforehand.

Authorised to receive the information is the person or persons who need(s) the information in order to be able to carry out their work and who have been screened for secrecy.

Professional secrecy undertakings Professional secrecy undertakings shall be entered into with all persons who are given information that is classified as restricted or higher, and when entered into shall apply for the whole of OKG.

Reclassification of information at OKG

Reclassification can be performed at the request of the person responsible for the information.

Exchange of information with authorities

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

Exchange of information with other external parties

There are handling rules used when exchanging secrecy classified information with external parties that shall be met. These describe the responsibilities and activities both in regards to receiving the information and sending it via various medium. The purpose of this is to secure maintained secrecy for the external parties and for OKG.

USB-memory - restrictive handling must be obtained, please see instruction 2007-21444E ” *Regulations for IT Security*”.

Marking

Documents are marked so that the recipient is given a clear indication that special handling rules 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 unauthorized distribution.

Information that is newly produced or revised /updated internally shall, irrespective of secrecy class, with the exception of secrecy class public, always be marked by using models in applications or stamping.

Handling of already existing technical information with the secrecy classes restricted and confidential, which previously have not marked, shall be known through knowledge.

Secrecy classification of information

Information shall always be classified for secrecy and be marked when it is created or received.

Secrecy classes:

- **Public** (Swedish “Öppen”)
- **Restricted** (Swedish “Intern”)
- **Confidential** (Swedish “Intern med begränsad spridning”)
- **Secret** (Swedish “Hemlig”)
- **Top secret** (Swedish “Kvalificerat hemlig”)

Public

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

Restricted

Restricted information is of the type such that its distribution, unauthorised use or change in it would lead to restricted or minor damage to the company or a person.

Physical storage

May be stored openly on OKG’s premises but protected against unauthorised access. Outside OKG, restricted information shall be kept under observation or stored in a locked space.

Electronic storage

Shall take place in a controlled way so that only authorised personnel are allowed access to the information.

Distribution

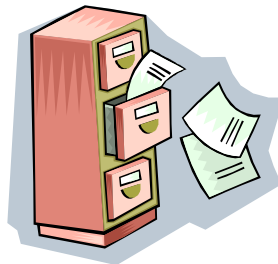
Allowed to be distributed within OKG. External distribution is allowed **if** the recipient is authorised.

Destruction

Information in paper form with security class restricted shall be processed through the paper recycling system. Outside OKG information shall be destroyed so that unauthorized distribution not occurs.

Electronic destruction

For storage media in which deletion is not possible, e.g. CD/DVD, physical destruction shall be performed.



Confidential

Type of information that can be used as a source of information at the threat of a sabotage, attack, act of terror or theft of core subject or nuclear waste. All technical documentation is classified as confidential which also shall constitute the lowest secrecy class, however with exception specified in above-mentioned instruction. This even includes photos on technical installations and equipment at OKG. Also other information than technical documentation can be classified as confidential.

Physical storage

May be stored openly on OKG's premises but protected against unauthorised access. Outside OKG, the information shall be stored in a secure way in a safe, in a burglar-proof data media cabinet, in a box for valuables that is classified to burglary class SS 3492 or in a burglar-proof filing cabinet.

Electronic storage

OKG is required to make a review of the external company's IT environment with respect to information and IT security. This review shall then be presented to and approved by the Information and IT Security Forum.

Distribution

Allowed to be distributed within OKG and applies to paper media, e-mails and faxes. External distribution is allowed *if* the recipient is qualified, for example to collaborators. External information is sent as "Brev med tillägg - Värde/Letter with supplement - Value" together with a post office receipt

External distribution shall always have an accompanying letter. For unmarked information, the secrecy class must be concluded in the accompanying letter.

Electronic distribution

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

- encrypted e-mail
- encrypted file server solution

Destruction

Inside OKG processed through the paper recycling system. Outside OKG information shall be destructed in a document shredder with a so-called cross-cut function.

Electronic destruction

For storage media in which deletion is not possible, e.g. CD/DVD, physical destruction shall be performed.



Secret

Type of information that gives the company a clear advantage over its competitors and whose disclosure, distribution, use or change could be damaging for the company or an individual person.

Secret information may only be processed electronically in stand-alone computers. Print-outs may only be processed to stand-alone printers.

Physical storage

Shall be stored in a secure way in a safe, in a burglar-proof data media cabinet, in a box for valuables that is classified to burglary class SS 3492 or in a burglar-proof filing cabinet.

Electronic storage

If information is to be processed electronically externally, it must be done in a separate security network that has no connection with other networks. OKG shall also conduct a review of the network, which is then presented to and approved by the Information and IT Security Forum.

Distribution

May be sent by internal post with the following requirements:

- The information shall be sent in a sealed envelope with the recipient's address on it.
- The envelope shall then be placed in a circulation envelope.
- The sender must make sure that the recipient will be present before information is sent and also inform that there is incoming information on its way.
- The person who sends it shall document the name and number of the information and the recipient is informed by e-mail that it has been sent.
- On receipt, the recipient confirms that the information has arrived.

If receipt is not obtained by the sender within two days, then this shall immediately be reported to the Information Security Manager.

External distribution is allowed *if* the recipient is qualified, for example to collaborators. For external distribution the terms from the Swedish Post Office "Brev med tillägg – Värde/Letter with supplement - Value" shall be sent, together with notice of delivery.

Communication to a receiver that is not on the original distribution list shall be approved by the person responsible for the information and registered by the department for Information Management at OKG.

Electronic distribution

- Distribution via e-mail and fax is not allowed.
- Information should not be discussed over the phone.

Destruction

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

Electronic destruction

For storage media in which deletion is not possible, e.g. CD/DVD, physical destruction shall be performed.

Top secret

Information that can jeopardize the nation's safety and E.ON's future market positions. Can only be handled by the Security Protection Manager of OKG.