Information Security – Manual

This manual describes how we at OKG, for reasons of secrecy, handle documents. For detailed information, please refer to instructions 2011-02371E *Regulations for Information Security* 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 secrecy classification. The classification specifies the requirements that apply for storage, distribution, destruction etc.

Authorized to receive the information, are the individuals who need the information in order to be able to carry out their work, who have been security cleared, who have signed a confidentiality agreement and who have adequate knowledge of information security/security protection.

Reclassification of information at OKG

Reclassification may be performed at the request of the entity 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, request for maintained secrecy must be made for documents that are classified as confidential, secret or top secret.

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 memory sticks - restrictive handling must be applied, 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 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 unauthorized distribution.

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

Documentation that lack 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.

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

Classification levels:
- **Public** (Swedish "Öppen")
- **Restricted** (Swedish "Intern")
- **Confidential** (Swedish "Intern med begränsad spridning")
- **Secret** (Swedish "Hemlig", security classification Secret/Restricted)
- **Top secret** (Swedish "Kvalificerat hemlig", security classification Secret/Confidential)

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

Restricted
Restricted information is of the type by which its distribution, unauthorized 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 unauthorized access. Outside OKG, restricted 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 authorization management system.

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

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

Electronic destruction
Regarding storage media for which deletion is not possible, e.g. CD/DVD, physical destruction must be performed.

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 exceptions 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 unauthorized access. Outside OKG, the information must be stored in a secure manner within locked premises protected against unauthorized access.

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

Regarding electronic storage outside OKG, it is required that OKG conducts an audit of external companies' premises, IT environments and the like.

Distribution
May be distributed within OKG. External distribution is permitted ***provided that*** the recipient is authorized. 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 up in such a manner that unauthorized 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)

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
Regarding storage media for which overwriting by the use of DBAN is not possible, or any other kind of method approved by the IT security manager, such as CD/DVD, physical destruction must be performed.

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

Physical storage
Must be stored by a secure method in a safe, in a burglar-proof data media cabinet, in a box for valuables classified in accordance with burglary classification Swedish Standard SS 3492 or SSF 3492, or in a burglar-proof filing cabinet.

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.

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 authorized. 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 up in such a manner that unauthorized 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 entity responsible for the information and be recorded by updating the distribution list.

Electronic distribution
Internal distribution at OKG is primarily performed via the application named Secret Oden. Distribution by the use of CD, DVD or USB memory stick approved by OKG may take place, provided that the above-mentioned regulations for physical distribution are complied with. 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
Regarding storage media for which overwriting by the use of DBAN is not possible, or any other kind of method approved by the IT security manager, such as CD/DVD, physical destruction must be performed.

Top secret
Information classified as Secret/Confidential, which may result in not insignificant damage to the national security of Sweden in the event of disclosure. Top secret information is stored at the Security Manager’s office at OKG.