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, handling, distribution, etc.

OKG may only request from other companies and authorities along with individuals that they must protect our information, provided that it has been classified by us.

Authorized to receive the information, with the exception of classification level Public, are the individuals who need the information in order to be able to carry out their work, who have been security cleared, and who have signed a confidentiality agreement.

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 documents. 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. Furthermore, there are handling regulations in use that must be observed when exchanging classified information with external parties. These describe the responsibilities and activities both with respect to receiving as well as sending information via various media. The purpose of this is to secure maintained secrecy for the external parties as well as for OKG.

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.

Handling of existing technical documentation classified as restricted or confidential, which previously have not been marked, shall be known through knowledge.

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")
- **Top secret** (Swedish "Kvalificerat hemlig")

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 on 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
Must take place in a controlled manner so that only authorized personnel are allowed access to the information.

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

Destruction
At OKG, information is processed through the normal paper recycling system. Outside OKG, information must be destructed so that unauthorized distribution does not occur.

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. This also includes photos of technical installations and equipment at OKG. 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 on 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
OKG is required to make a review of the external company's IT environment with respect to information and IT security. This review must then be presented to and approved by the Information and IT Security Forum.

Distribution
May be distributed within OKG. External distribution is allowed ***provided that*** the recipient is authorized. The information is sent as "Brev med tilläggstjänst –Rek alternativt Värde" (Letter with additional services – Registered mail alternatively Valuables) together with a proof of receipt in accordance with the PostNord Sverige AB's specific conditions for "Letter with additional services". At OKG, external distribution including bookkeeping and making sure that the letter 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 e-mail
- encrypted file server solution

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 deletion is not possible, e.g. 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 vital to the national security.

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 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, which is then approved by the Information and IT Security Forum.

Distribution

May be sent by internal post at OKG with the following requirements:

- The information must be sent in a sealed envelope with the recipient's address on it.
- The envelope must then be placed in a circulation envelope.
- The sender must make sure that the recipient will be present before the information is sent and also inform that an item of mail is on its way.
- The person who sends the information must document the name, the dispatch date and the registration number of the item of mail or similar information. The information is saved until the sender has made sure that the item of mail has reached its recipient.
- The recipient must confirm that the information has arrived.

Should the sender not receive the receipt for the dispatched information within one week, he/she must report this to the Information Security Manager accordingly, who assesses any possible damage.

External distribution is permitted provided that the recipient is authorized. The information is sent as "Brev med tilläggstjänst –Rek alternativt Värde" (Letter with additional services - Registered mail alternatively Valuables) together with a proof of receipt in accordance with the PostNord Sverige AB's special conditions. At OKG external distribution including bookkeeping and making sure that the letter reaches the recipient is handled by subsection Shared Services, Administration, Service.

Communication to a recipient that is not on the original distribution list must be approved by the entity responsible for the information and registered by the Information Management Section at OKG.

Electronic distribution

- Internal distribution at OKG is primarily performed via the application named Secret Oden.
- Distribution via CD, DVD or USB memory stick approved by OKG may take place, provided that the above-mentioned regulations for physical distribution are applied.
- 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 deletion is not possible, e.g. CD/DVD, physical destruction must be performed.

Top secret

Information which contains data of exceptional importance to the national security and information that must be kept secret with respect to Uniper's future market positions. Top secret information is stored at the Security Manager's office at OKG.