

## 8. MODULE FOR ACCESS CONTROL AND USER MANAGEMENT

### 8.1 Purpose of module

This module is used to control access to reading, registering and updating various kinds of information which is stored in the database.

The system is to provide for the management of users and their association with administrative units. It should differentiate the individual users' read and right access- both with regard to their administrative ties and their roles and responsibilities as managers and executive officers.

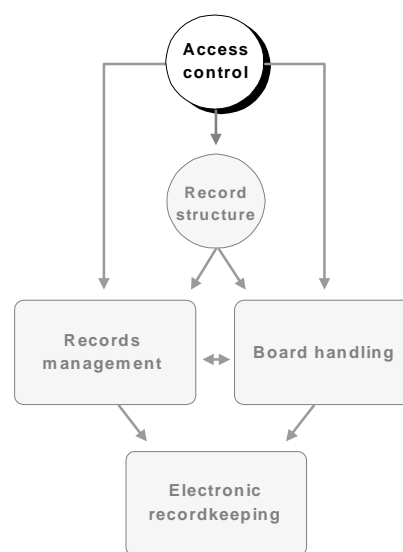
The system should have functions for screening information which is to be subject to provisions concerning exemption from public access and the protection of personal integrity, etc. This should make it possible to regulate public access to records information and case documents, in accordance with the provisions of the Freedom of Information Act.

The main purpose of the module may be summarized as follows:

- To ensure that the right person in the right position is given the access necessary to perform tasks
- To prevent intruders from gaining access to screened-off information
- To guarantee the public's statutory right to access to information

Electronic case handling and recordkeeping provides for changes in the division of labour between executive officers and the centralized recordkeeping services. New functions for registration and storage - of drafts, notes, remarks, logging of document flow and finalized case documents - are intimately connected with the production process itself, and presuppose that executive officers contribute in a more direct way than before. Such contribution is in many areas necessary in order to implement the new functions. Increased opportunities for the executive officers to carry out the registration and updating themselves may, however, increase the risk of having incorrect or incomplete information registered in the system, and possibly of reducing data integrity. In order to prevent such consequences from the increased delegation of responsibility and authority, the system has been enhanced with several new *quality-control functions*:

- more detailed access control
- stricter process-management procedures which regulate when and in what order the individual users perform their registration tasks



**Figure 8-1: Position of access-control module in Noark**

- identification of the persons responsible for performing specific tasks
- logging of completed changes in well-defined function areas
- centralized verification of performed tasks and registered information

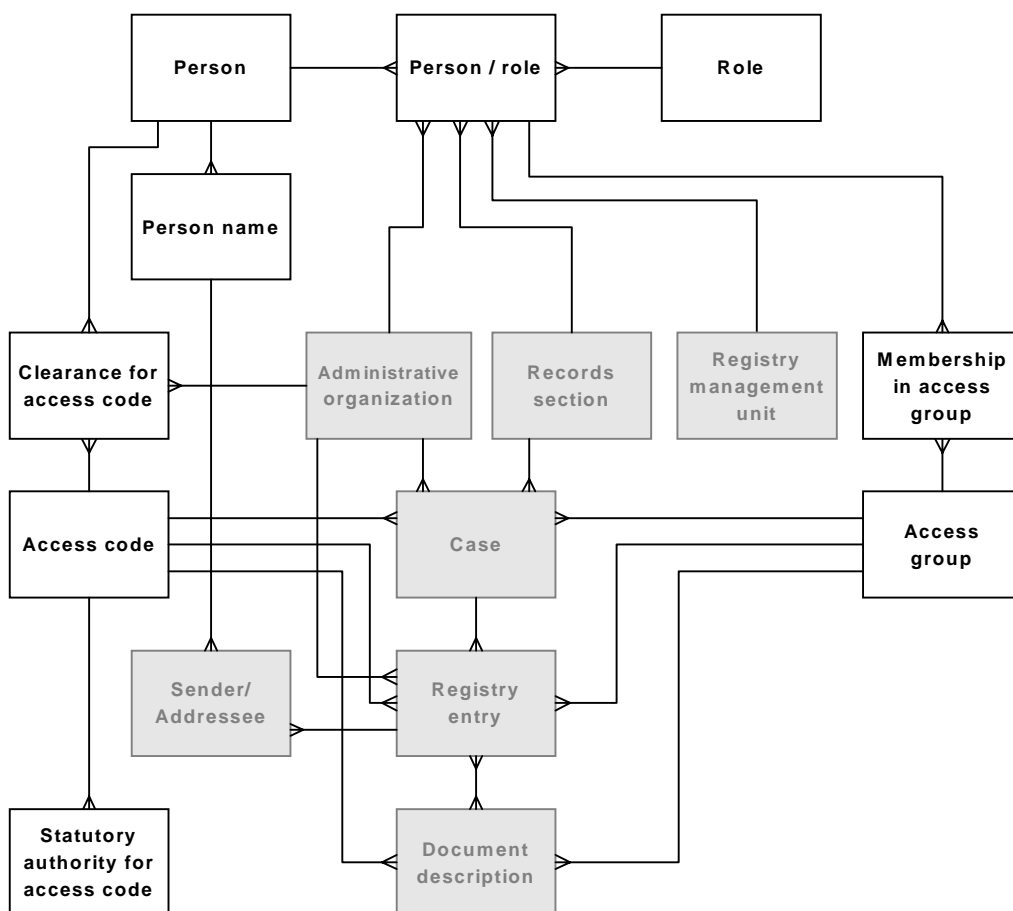
## 8.2 Module design

The essential tables in this module are *Person*, *Person-Role* and *Role*. *Person* describes all the persons within the organization who have rights within the system, persons who have had rights within the system and persons to whom references are made from one or more records within the system (as executive officer, board member, etc.). The table *Person* also handles history with regard to name changes, etc., by linking up to *Person name*. *Person-Role* associates a person with a role, and *Role* contains information on the rights associated with the individual roles.

Other important tables are *Clearance for access code*, which authorizes users for access to screened information, and *Membership in access group*, which makes it possible to screen the information access to specified groups of users according to need.

The following figure shows important tables included in the module as white boxes. The gray boxes are tables from other modules which are necessary for demonstrating the logic of the system.

**Figure 8-2: Module for access control and user management**



## 8.2.1 User management

The user management is a basic security function in the Noark system. It determines what functions may be performed by whom, which is essential to the data quality of the base. It also determines who gets access to what information. This must function adequately for it to be advisable to register and store sensitive information in the base. The following general requirements apply to the user administration in Noark-4:

K8.1	The module for access control and user management should control and survey all use of the system. The users should only be able to use functions and information for which they are authorized. Authorization and verification is controlled by the information content in the tables of the module.	O
K8.2	At logon, all users should identify themselves by a user identification controlled by the system. The user identification should give the system the necessary access to information concerning the user's rights and restrictions.	O
K8.3	The functions to which the user has access should, as far as possible and appropriate, appear from the individual panels (e.g., through the use of different colours, shades of grey, etc., on icons).	A
K8.4	The same person (user) should be able to use different names and initials, e.g., after changing his/her name. It should be possible to preserve all names and initials in the system as well as information on periods of use. The system should keep track of names and initials which belong to the same person (see the tables <i>Person</i> and <i>Person name</i> ).	O
K8.5	It should be possible to decide that a person (secretary) may register on behalf of somebody else, and with the same rights as that person.	A
K8.6	The system should always provide for "alias" searches for all names and initials associated with a person. Searches for names should, in such cases, include all names associated with the person concerned. It should also be possible to disable the "alias" function.	A

The rights and restrictions of the users are associated with their roles:

K8.7	A user of the system should be associated with one or more roles, each giving specific rights. The user's association with a role should be limited to a specific period of time (from date to date).	O
K8.8	The user's right in connection with a role should be defined globally, i.e., for the entire database, or within a registry management unit.	O1
K8.9	One of the roles with which the user is associated, should be defined as his/her normal role, i.e., the role which the user will play unless otherwise specified.	O
K8.10	It should be possible to associate a person in a specific role with an administrative unit, a registry management unit and a records section (table: <i>Person-Role</i> ). It should be possible to use these units as default values when the user performs registrations which involve these attributes.	O

## 8.2.2 Managing write access

Write access in the Noark base includes the right to:

- register and modify information
- perform specific functions, such as create a new case or registry entry, etc.

Write access is managed through:

- general rights and restrictions associated with individual roles
- rights and restrictions for the individual roles at the various process stages of the document handling (see chapter 6).

### 8.2.2.1 Roles and associated rights

Noark-4 defines a set of default roles with specific rights and restrictions. It should, however, be possible to introduce further differentiation according to the needs of the organization.

K8.11	<p>As a default, the following roles should be defined in the system (the corresponding user types in Noark-3 and Koark are indicated in brackets):</p> <p><i>Role 0 - SY</i>: System administrator (Koark: 0)</p> <p><i>Role 1 - AR1</i>: Registry administrator (Koark: 1, Noark-3: 1)</p> <p><i>Role 2 - AR2</i>: Registry personnel (Koark: 2)</p> <p><i>Role 3 - LD</i>: Manager/case distributor (Koark: 3, Noark-3: 2)</p> <p><i>Role 4 - SB</i>: Executive officer (Koark: 4, Noark-3: 3)</p> <p><i>Role 5 - US</i>: Board secretary (Koark: 5)</p> <p><i>Role 6 - AN</i>: Other (Koark: 6, Noark-3: 4).</p> <p><i>Role 7 - EKS</i>: External (Koark: included in 6, Noark-3: included in 4).</p> <p><i>Role 5</i> only applies to the board-handling module (<i>requirement type U</i>).</p> <p><i>Role 7</i> only applies when the recommended functions for giving external users access to the base, have been included, cfr. K8.89 - K8.90 (<i>requirement type A</i>).</p>	O
K8.12	It should be possible to define other roles in addition to these. When this is done, it should be possible to use a default role as starting point and then edit it.	O1
K8.13	It should be possible to register the individual rights which may be associated with a role, in separate attributes, in accordance with the specifications in the table <i>Role</i> , or by other means which provide similar flexibility.	O1
K8.14	It should not be possible to create roles which unblock the general restrictions of the system.	O

The following general rights and restrictions should be associated with the individual default roles (note that all rights are limited by the restrictions associated with the individual attributes in chapter 14):

K8.15	<p><i>Role 0 - SY (System administrator):</i></p> <ul style="list-style-type: none"> <li>• Rights:                     <ul style="list-style-type: none"> <li>- access to all system and operating functions</li> <li>- the right to authorize himself/herself and other users for all types of rights</li> </ul> </li> <li>• Restrictions:                     <ul style="list-style-type: none"> <li>- no access to registration and correction functions in the records management module, electronic recordkeeping, record structure module and board-handling module</li> </ul> </li> </ul>	O
K8.16	<p><i>Role 1 - AR1 (Registry administrator):</i></p> <ul style="list-style-type: none"> <li>• Rights:                     <ul style="list-style-type: none"> <li>- permission to create cases, registry entries and electronic documents</li> <li>- permission to file and dispatch electronic documents</li> <li>- access to all registration and correction functions (including moving registry entries) in the records management module, electronic records and record structure module</li> <li>- the right to authorize himself/herself and other users for registering in the same three modules, as well as access codes and association with access groups</li> <li>- the rights apply to the entire Noark base</li> </ul> </li> <li>• Restrictions:                     <ul style="list-style-type: none"> <li>- the authorization right for access codes only applies to the codes for which the person himself/herself is authorized</li> <li>- the right to register and make corrections is restricted by the process-management rules (see below)</li> <li>- the right to register and make corrections in the electronic records does not include the right to modify filed documents</li> </ul> </li> </ul>	O
K8.17	<p><i>Role 2 - AR2 (Registry personnel):</i></p> <ul style="list-style-type: none"> <li>• Rights:                     <ul style="list-style-type: none"> <li>- permission to create cases, registry entries and electronic documents</li> <li>- permission to file and dispatch electronic documents</li> <li>- access to all registration and correction functions (including moving registry entries) in the records management module and electronic records</li> <li>- permission to associate users with access groups</li> </ul> </li> <li>• Restrictions:                     <ul style="list-style-type: none"> <li>- the right to register and make corrections is restricted by the process-management rules (see below)</li> <li>- the right to register and make corrections in the electronic records does not include the right to modify filed documents</li> <li>- all registration functions and write access are limited to the person's own registry management unit</li> </ul> </li> </ul>	O

K8.18	<p><i>Role 3 - LD (Manager/case distributor):</i></p> <ul style="list-style-type: none"> <li>• Rights:                     <ul style="list-style-type: none"> <li>- permission to create cases, registry entries and documents</li> <li>- access to registration and correction functions in the records management module and electronic records according to the process-management rules (see 8.2.2.2 and chapter 6)</li> <li>- permission to register notes</li> <li>- permission to register handling plan for board handling in a case</li> <li>- the right to authorize executive officers for registration in accordance with the rights and restrictions of role 4 - SB (cfr. K8.19), as well as for access codes and membership in access groups</li> </ul> </li> <li>• Restrictions:                     <ul style="list-style-type: none"> <li>- the authorization right for access codes only applies to the codes for which the person himself/herself is authorized</li> <li>- the right to create registry entries is limited to cases associated with the person's administrative unit or units subordinate to it, or to cases where there already exist registry entries associated with this/these unit(s)</li> <li>- all other registration functions and write access are limited to the person's own registry management unit or units which are subordinate to it.</li> </ul> </li> </ul>	O
K8.19	<p><i>Role 4 - SB (Executive officer):</i></p> <ul style="list-style-type: none"> <li>• Rights:                     <ul style="list-style-type: none"> <li>- permission to create cases, registry entries and documents</li> <li>- access to registration and correction functions in the records management module and electronic records according to the process-management rules (see 8.2.2.2 and chapter 6)</li> <li>- permission to register notes</li> <li>- permission to register handling plan for board handling in a case (for which the person is case-responsible)</li> <li>- the right to create ad-hoc access groups associated with cases for which the person is case-responsible, or with registry entries for which the person is executive officer</li> </ul> </li> <li>• Restrictions:                     <ul style="list-style-type: none"> <li>- the right to create registry entries is limited to cases for which the person is case-responsible, or to cases where there are already registry entries for which the person is executive officer</li> <li>- all other registration functions and write access are limited to cases for which the person is case-responsible, or to registry entries and their associated documents for which the person is executive officer</li> </ul> </li> </ul>	O

K8.20	<p><i>Role 5 - US (Board secretary):</i></p> <ul style="list-style-type: none"> <li>• Rights:                     <ul style="list-style-type: none"> <li>- access to all functions for registering, correcting, filing, etc., in the board-handling module</li> <li>- the same rights as SB for document type S in the records management module and electronic records (see below concerning process management)</li> <li>- permission to register notes</li> </ul> </li> <li>• Restrictions:                     <ul style="list-style-type: none"> <li>- the registration functions and write access in the board-handling module are limited to the board(s) for which the person is registered as secretary</li> <li>- the write access in the board-handling module is limited to the documents for which the person is registered as executive officer</li> </ul> </li> </ul>	U
K8.21	<p><i>Role 6 - AN (Other),</i>  <i>Role 7 – EKS (External): No write access</i></p>	O

*Note: K8.15 – K8.19 as well as K8.21 are designated type O, even if they also refer to some modules and functions which are not included in the basic version of Noark-4. This means that the rights in question must be considered obligatory where relevant. For instance, requirements concerning notes and electronic records are to be considered as O2 requirements.*

### 8.2.2.2 Rights at various process stages in document processing

Chapter 6 describes various process courses in connection with document handling, what parties are involved and what rights and responsibilities they have at various stages of the handling process. The description uses the process itself as its starting point and place the various parties with their rights and responsibilities in relation to this. This chapter starts off from the individual persons involved and summarizes their rights and restrictions at various stages of the process.

Chapter 6 operates with three types of parties (persons) in connection with document handling. They correspond to the above user roles as follows:

- AR (registry office) includes both AR1 and AR2 (roles 1 and 2). They have the same rights in the handling process, but the rights of AR2 are generally limited to his/her own registry management unit, while AR1 may operate in the entire Noark base.
- LD (manager) corresponds to the role of LD (role 3).
- SB (executive officer) corresponds to the role of SB (role 4). Note that US (role 5) has the same rights as SB for document type S.

The following description uses the designations AR, LD and SB. Their general rights and restrictions follow the specification of requirements in 8.2.2.1 above.

Process-related rights and restrictions for AR (roles AR1 and AR2):

K8.22	Case status = R, B, X	The general rights and restrictions for AR apply in their entirety.	O
K8.23	Case status = A	The following restrictions in the general rights apply to AR: <ul style="list-style-type: none"> <li>• AR may only modify the following attributes in or associated with the table <i>Case</i>: <ul style="list-style-type: none"> <li>- <i>Case status</i></li> <li>- attributes for access control</li> <li>- attributes for precedent</li> <li>- attributes for disposal</li> <li>- attributes associated with <i>Cfr. case</i></li> <li>- <i>(Re)activation (date)</i></li> <li>- lending attributes</li> <li>- <i>Records section</i> (only as part of a move according to the specifications of K12.5 and K12.6)</li> </ul> </li> <li>• AR may not create new registry entries in the case or associate new electronic documents.</li> <li>• AR may not dispatch or file electronic documents associated with the case.</li> </ul>	O
K8.24	Case status = U	AR may modify the attribute <i>Case status</i> . All other registration functions are blocked.	O
K8.25	Registry status = M, S, R, F, E, J	The general rights and restrictions for AR apply in their entirety.	O1
K8.26	Registry status = A	The following restrictions in the general rights apply to AR: <ul style="list-style-type: none"> <li>• AR may only modify the following attributes in or associated with the table <i>Registry entry</i>: <ul style="list-style-type: none"> <li>- <i>Registry status</i></li> <li>- Attributes for access control</li> <li>- Attributes for lending</li> <li>- <i>Records section</i> (only as part of a move according to the specifications of K12.5 and K12.6)</li> </ul> </li> <li>• AR may not associate new electronic documents with the registry entry.</li> <li>• AR may not dispatch or file electronic documents associated with the case.</li> </ul>	O1
K8.27	Registry status = U	AR may modify <i>Registry status</i> , but has no registration rights beyond this.	O1
K8.28	Document status = B (or equivalent)	AR has no registration rights in the tables <i>Document description</i> and <i>Version</i> .	O2
K8.29	Document status = F	The general rights and restrictions for AR apply in their entirety.	O2

*Process-related rights and restrictions for LD and SB:*

K8.30	Case status = R	Process-related rights for LD and SB: <ul style="list-style-type: none"> <li>• The general rights and restrictions apply.</li> <li>• LD/SB may register in all attributes in the tables <i>Case</i> and <i>Part in case</i> (if implemented).</li> </ul>	O
K8.31	Case status = B, X	Process-related rights for LD and SB: <ul style="list-style-type: none"> <li>• LD/SB may modify the following attributes in or associated with the table <i>Case</i>: <ul style="list-style-type: none"> <li>- attributes in <i>Part in case</i> (if implemented)</li> <li>- attributes associated with <i>Cfr. case</i></li> <li>- attributes for access control</li> <li>- attributes for precedent</li> <li>- <i>(Re)activation (date)</i></li> </ul> </li> <li>• LD/SB may create new registry entries in the case.</li> </ul>	O
K8.32	Case status = A	Process-related rights for LD and SB: <ul style="list-style-type: none"> <li>• LD/SB may modify the following attributes in or associated with the table <i>Case</i>: <ul style="list-style-type: none"> <li>- attributes for access control</li> <li>- attributes for precedent</li> <li>- <i>(Re)activation (date)</i></li> </ul> </li> </ul>	O
K8.33	Case status = U	LD/SB do not have access to registration functions in the case.	O
K8.34	Registry status = M	Process-related rights for LD and SB: They may register in all attributes in the tables <i>Registry entry</i> and <i>Sender/Addressee</i> .	O1
K8.35	Registry status = S, R	Process-related rights for LD and SB: <ul style="list-style-type: none"> <li>• LD/SB may register in all attributes in the tables <i>Registry entry</i> and <i>Sender/Addressee</i>.</li> <li>• LD/SB may associate electronic documents with the registry entry.</li> </ul>	O1
K8.36	Registry status = F	Process-related rights for LD and SB: <ul style="list-style-type: none"> <li>• LD/SB may modify the following attributes in the tables <i>Registry entry</i> and <i>Sender/Addressee</i>: <ul style="list-style-type: none"> <li>- <i>Registry status</i> (to the values <b>R</b> or <b>E</b>)</li> <li>- attributes for access control</li> <li>- <i>Executive officer</i> (only LD)</li> <li>- <i>Maturity date</i> and <i>Processing deadline</i> (only LD)</li> <li>- attributes for depreciation</li> </ul> </li> <li>• LD/SB may dispatch and file electronic documents associated with the registry entry.</li> </ul>	O2
K8.37	Registry status = E	Process-related rights for LD and SB: <ul style="list-style-type: none"> <li>• LD/SB may modify the following attributes in the tables <i>Registry entry</i> and <i>Sender/Addressee</i>: <ul style="list-style-type: none"> <li>- <i>Registry status</i> (to the values <b>R</b> or <b>F</b>)</li> <li>- attributes for access control</li> <li>- <i>Executive officer</i> (only LD)</li> <li>- <i>Maturity date</i> and <i>Processing deadline</i> (only LD)</li> </ul> </li> </ul>	O2

		<ul style="list-style-type: none"> <li>- attributes for depreciation</li> <li>• LD/SB may dispatch to CC addressees and file electronic documents associated with the registry entry.</li> </ul>	
K8.38	Registry status = J	Process-related rights for LD and SB: <ul style="list-style-type: none"> <li>• LD/SB may modify the following attributes in the tables <i>Registry entry</i> and <i>Sender/Addressee</i>:               <ul style="list-style-type: none"> <li>- attributes for access control</li> <li>- <i>Executive officer</i> (only LD)</li> <li>- <i>Maturity date</i> and <i>Processing deadline</i> (only LD)</li> <li>- attributes for depreciation</li> </ul> </li> </ul>	O1
K8.39	Registry status = A	Process-related rights for LD and SB: <ul style="list-style-type: none"> <li>• LD/SB may modify the following attributes in the table <i>Registry entry</i>:               <ul style="list-style-type: none"> <li>- attributes for access control</li> </ul> </li> </ul>	O1
K8.40	Registry status = U	No registration rights for LD/SB.	O1
K8.41	Document status = B (or equivalent)	Process-related rights for LD and SB: They may register in all available attributes in the tables <i>Document description</i> and <i>Version</i> as well as file new versions of the document.	O2
K8.42	Document status = F	Process-related rights for LD and SB: <ul style="list-style-type: none"> <li>• LD/SB may modify the following attributes in the table <i>Document description</i>:               <ul style="list-style-type: none"> <li>- <i>Document status</i> (on certain conditions - see K6.30)</li> <li>- attributes for access control</li> </ul> </li> </ul>	O2

### 8.2.3 Managing read access

The access control of Noark-4 regulates the read access to the information in the database. This applies to all kinds of information - records management information (including records information), documents in the electronic records and all kinds of background information concerning administrative structure, record structure, user roles, etc.

Noark-4 assumes that the information in the base is open to all users. However, it contains several functions for screening of information to which not everybody should have access. Such screening may be relevant for information which is subject to exemption from public access according to laws and regulations, and it may be resorted to for information which the organization - for other reasons - prefers not to distribute to all its users.

Screening of information is closely related to the provisions of the Freedom of Information Act and its regulations. The access control of Noark-4 is designed with an eye on these provisions, and it provides the necessary flexibility to carry out the screening according to the letter and intention of the act. The way in which the screening is carried out, however, cannot be governed by Noark. It will depend on the procedures set up by the individual user organization and the way in which the users (managers, registry personnel, etc.)

practise the established procedures. This is discussed in more detail in paragraph 8.3.3 below.

The provisions of the Freedom of Information Act regulate *public* access to records information and case documents. However, the way in which a public body regulates access to information for the *users in the Noark system* (hereafter referred to as internal users), is not covered by the Freedom of Information Act. This is up to the organization itself, as long as any provisions on confidentiality, protection of personal integrity, etc., are respected.

In the context of Noark, it seems natural to emphasize the importance of giving as many internal users as possible access to the information in the base (that which is not subject to professional secrecy). However, there may also be organizations which need to limit read access, especially for internal documents and other internal information, to those parts of the records base which are associated with the users' own administrative or record-organizational unit(s). This may for instance apply to large or complex organizations which share a Noark base, such as a state office which covers the entire country, the entire local administration of a large district council, etc. In some cases, such limitation may be necessary in order not to be subject to licensing according to the Personal Data Registers Act, cfr. the *Personal Data Registers Regulation, § 2-19 on electronic records*.

This sub-chapter deals with the management of read access in the records management module and electronic records. The read access in the board-handling module are discussed as part of a complete presentation of that module in chapter 9.

### 8.2.3.1 Screening functions in a Noark system

There are two principles for screening in Noark-4:

1) *Screening based on access codes (corresponds to "grad-koder" (grading codes) in Noark-3 and Koark):*

This is used to screen registered information or individual documents. The screening enters into force when an access code is applied to an individual case, registry entry or document. The system users must be *cleared* for specific access codes and *authorized* for a defined part of the cases and registry entries and their associated documents which are screened using individual access codes. Only users who are cleared for a specific access code and authorized for the concerned case and/or registry entry, may see the information which is screened using this code. The information to be screened in a case, registry entry or document is indicated by checking off, cfr. 8.2.3.3 below. All other information is open to everybody (within the context of access according to administrative or record-organizational criteria - see no. 2 below). The access codes to be used are described in paragraph 8.2.3.2.

Within the framework of the individual access code, the following opportunities exist for *authorizing* users (cfr. the table *Clearance for access code*):

- The default, which is implicit in the *clearance* for an access code, is that the user is authorized for information and documents within the cases for which he/she is case-responsible, as well as for information and documents in registry entries for which he/she is executive officer.

- The authorization may be extended by authorizing the user for information and documents within one or more administrative units as well as those units which are subordinate to them. The authorization may be defined in different ways for different access codes.
- The authorization may be further extended by associating the user with an *access group* and by using this access group in combination with the person's access code. Access groups are used to authorize users for access to individual cases, registry entries or documents across the administrative organization, case-responsibility, etc. Access groups may be defined on a general basis (e.g., »security board«), and an arbitrary number of cases, registry entries or documents may be associated with them. Access groups may also be defined ad hoc and be associated with a specific case or registry entry.

2) *Screening based on administrative or record-organizational criteria:*

This screening function should make it possible to limit the read access of the user to specific parts of the Noark base. The rights may be limited according to record-organizational criteria, based on the *registry entry*, or according to other administrative criteria, i.e., based on the *administrative unit including subordinate units*. Within the specified units, the user is given access to all information and all documents, with the restrictions that follow from the access codes and the authorization associated with these, cfr. no. 1 above. Outside the specified units, all information is blocked for the user.

Noark-4 does not pose specific requirements with regard to the layout of such a solution, or to whether record-organizational or administrative criteria should be used. The only requirement is that there should be a solution which makes it possible to limit read access to specific parts of the base according to general record-organizational or administrative criteria, cfr. K8.53.

It is up to the organization itself to decide what screening functions should be implemented. However, it is not recommended to use more functions than necessary. In small organizations, it will usually suffice to use access codes, especially if there is not a lot of sensitive information. For large organizations which process much and varied sensitive information, on the other hand, it may be appropriate to combine several screening functions.

*Note: When an executive officer or manager is given access to specific registry entries (with their associated documents) which are associated with units outside the person's authorization, the simplest thing will often be to define the person as CC addressee, cfr. paragraph 4.2.6. This may result in the person obtaining status as executive officer for the specific registry entry and thus read access to information and documents, within the framework provided by the access code.*

The system should provide for the following general functions for managing read access:

K8.43	It should be possible to register access codes for cases, registry entries and documents. The code indicates that registered information or filed documents should be screened against unauthorized access. The information to be screened and the ways of indicating this are specified in paragraph 8.2.3.3.	O
K8.44	It should be possible to <i>clear</i> an individual user for one or more access	O

	codes, cfr. the table <i>Clearance for access code</i> . In the basic version of Noark-4, users who are cleared for an access code should automatically be <i>authorized</i> to see all information which is screened with this code, possibly limited to the record-organizational or administrative units which are specified in accordance with K8.53. Users who are not cleared for an access code, may not read information screened with this code. This also applies to previously registered information if a user's clearance is withdrawn for the access code in question.	
K8.45	In an enhanced version of Noark-4, users who are cleared for an access code, should always be <i>authorized</i> for this within parts of the Noark base, cfr. the table <i>Authorization within administrative unit</i> . The authorization should be defined according to one of the following options: <ul style="list-style-type: none"> <li>• <i>Default authorization</i>, limited to cases for which the user is case-responsible or registry entries for which he/she is executive officer (both including associated information and documents). Default authorization is set automatically when the user is cleared for the access code.</li> <li>• <i>Enhanced authorization</i>, limited to one or more administrative units and the units subordinate to them. If the authorization is to apply to the entire organization, the organization should be defined as administrative unit.</li> </ul>	O1
K8.46	It should be possible to register a user as member of an access group, cfr. the table <i>Membership in access group</i> , and it should be possible to associate cases, registry entries and documents with an access group, cfr. the attribute <i>Access group</i> in the respective tables. Membership in an access group should authorize a user for access to information in those cases, registry entries and documents which are associated with the group, provided that the user is cleared for the access code indicated on the case, registry entry or document.	O1
K8.47	It should be possible to carry out the registration of access groups and membership in these, i.e., adding or removing members, in a separate operation. It should also be possible to carry out such registration in connection with the registration or correction of information in a case or registry entry.	O1
K8.48	A user should not be able to enter access codes for which he or she is not cleared himself/herself. Neither should the user be able to register or correct information in cases, registry entries or document descriptions for which he/she is not authorized.	O
K8.49	The system should prevent a case from having a case-responsible assigned who is not cleared for the access codes which are used in the case (including associated registry entries and documents, etc.). Likewise, the system should prevent a registry entry from having an executive officer assigned who is not cleared for the access codes used in the registry entry (including associated documents, etc.).	O
K8.50	As long as a case is not finalized (i.e., as long as <i>Case status</i> is different from <b>A</b> ), the system should prevent the case (including associated registry entries and documents, etc.) from having an access code assigned for which the case-responsible is not cleared. When <i>Case status</i> is <b>A</b> , the system should allow such registration, but only after the	O

	user has provided a confirmatory answer to a control question.	
K8.51	As long as a registry entry is not finalized (i.e., as long as <i>Registry status</i> is different from <b>A</b> ), the system should prevent the registry entry (including associated documents, etc.) from having an access code assigned for which the executive officer is not cleared. When <i>Registry status</i> is <b>A</b> , the system should allow such registration, but only after the user has provided a confirmatory answer to a control question.	O
K8.52	If a user's authorization or clearance is withdrawn, the system should issue a warning if the concerned person loses his/her access to cases/registry entries for which he/she is case-responsible or executive officer. If any of the cases or registry entries are not finalized, a confirmatory answer must be given to a control question before the change can be effectuated.	O1
K8.53	It should be possible to limit a user's read access to parts of the Noark base according to record-organizational criteria (one or more registry management units) or according to administrative criteria (one or more administrative units including subordinate units). It is optional whether both types of criteria should be permitted or only one type.	O1

### 8.2.3.2 Access codes and their statutory authority

The use of an access code for a case, registry entry or document has the following consequences:

- certain information is unavailable to internal users who are not cleared for the code in question
- this information is not included in the public registry, cfr. 8.2.3.5 below

It follows from the last indent that any use of access codes must be warranted in the Freedom of Information Act, and that it must be possible to indicate the statutory authority at request.

Noark-4 leaves it up to the individual organization to define what access codes will be used. However, all access codes should be registered in the system (by users who are authorized for such registration) before they are used, and they should relate to a statutory authority based on §§ 4, 5, 5a, 6 or 11 of the Freedom of Information Act.

K8.54	For it to be permissible to assign an access code to a case, registry entry or document, the code must be predefined (registered) in the system, cfr. the table <i>Access code</i> .	O
K8.55	Access codes which are defined in the system, are not valid unless there is a registered statutory authority for the code, cfr. the table <i>Statutory authority for access code</i> . Exempted from this requirement is access code XX (temporarily blocked), cfr. below.	O
K8.56	When an access code is registered for a case, registry entry or document, the system should automatically retrieve the corresponding statutory authority and add it to the relevant attribute of the case, registry entry or document. In order to remind the user that the automatically retrieved authority is not always complete, the prompt should be placed after the last character in the statutory authority field on the screen.	O

In Noark-4, some access codes and statutory authorities have been predefined. These codes should always exist in a Noark system, and they should (if possible) be blocked against changes. The codes are associated with fixed systems such as the safety instruction and the security and protection instruction as well as the individual paragraphs concerning exemptions in the Freedom of Information Act. Furthermore, a code has been added for temporary blocking information pending a decision as to whether the general public should have access to the information.

K8.57	The following access codes and their statutory authorities should be predefined in a Noark system. The individual organization should be able to add or remove codes according to need.	O
-------	---	---

<i>Code</i>	<i>Description</i>	<i>Statutory authority</i>
B	Restricted according to the Safety Instruction	Freedom of Information Act § 6.1, Safety Instruction
K	Confidential according to the Safety Instruction	Freedom of Information Act § 6.1, Safety Instruction
H	Secret according to the Safety Instruction	Freedom of Information Act § 6.1, Safety Instruction
F	"Fortrolig" (confidential) according to the Security and Protection Instruction	Freedom of Information Act § 5a, Security and Protection Instruction
SF	"Strengt fortrolig" (strictly confidential) according to the Security and Protection Instruction	Freedom of Information Act § 5a, Security and Protection Instruction
4	Public access delayed in accordance with the Freedom of Information Act, § 4 (to be specified)	Freedom of Information Act § 4
5	Exempt from public access in accordance with the Freedom of Information Act, § 5 (statutory authority must be further specified)	Freedom of Information Act § 5
5a	Exempt from public access in accordance with the Freedom of Information Act, § 5a (statutory authority must be further specified)	Freedom of Information Act § 5a
6	Exempt from public access in accordance with the Freedom of Information Act, § 6 (statutory authority must be further specified)	Freedom of Information Act § 6
11	Exempt from public access in accordance with the Freedom of Information Act, § 11 (statutory authority in regulation must be further specified)	Freedom of Information Act § 11
XX	Temporarily blocked	

K8.58	The codes B, K and H should be grouped together in a hierarchy with H on top and B at the bottom. This should result in all users who are authorized for H being automatically authorized for K and B, etc. A similar hierarchy should be defined for the codes F and SF, where SF is the highest.	A
K8.59	It should be possible to define similar hierarchies for other sets of access codes.	A

The codes 5, 5a and 6 are general codes for information which is exempt from public access according to the three paragraphs in the Freedom of Information Act. This may suffice for organizations which have little material for screening. However, in many cases it may be appropriate to use a higher number of more specialized codes for information to be screened, e.g., P for personnel cases, KL for client cases, etc. In this way, exemption from public access may be combined with screening from internal user groups (for instance so that only the personnel department and certain managers are authorized for code P, etc.).

When statutory authority is specified, the setup may be as follows:

<i>Code</i>	<i>Description</i>	<i>Statutory authority</i>
P	Personnel cases	Freedom of Information Act § 5a, Public Administration Act § 13.
KL	Client cases	Freedom of Information Act § 5a, Public Administration Act § 13.

On the other hand, it soon becomes difficult to keep track if too many different access codes are used. If there is a need for highly differentiated screening, it is recommended that differentiated authorization of users be used within the individual access codes, administratively or using access groups.

Access code XX is an exception. It is applied automatically by the system to all newly registered cases, registry entries and documents, and indicates that the information is blocked until a decision has been made with regard to public access/screening. This is described in more detail in 8.2.3.4. Code XX does not entail exemption from public access, only a temporary delay, in accordance with current good practice and without affecting the provisions of the Freedom of Information Act. No statutory authority has thus been specified for this code, cfr. K8.55 above.

### 8.2.3.3 Screening of individual pieces of information and documents

Screening based on *record-organizational or administrative criteria* includes all information in cases, registry entries and case documents which are not associated with the concerned units, cfr. K8.53 above. The screening enters into force the moment the administrative and/or record-organizational position of the case or registry entry is established.

Screening according to *access code* only applies to a set of information within the concerned case or registry entry, as well as any complete case documents. The access code is assigned when the case or registry entry is registered, or possibly later.

K8.60	It should be possible to screen the following case information using an access code: <ul style="list-style-type: none"> <li>• Parts of the case title (<i>Case title</i> in the table <i>Case</i>): the system should either permit the screening of everything but the first part of the title (e.g., the first line) or screening of individual words which the user highlights.</li> <li>• File codes/filing plan codes (<i>Order value</i> in the table <i>Filing plan code</i>): This is primarily intended for the screening of object codes which are person names.</li> <li>• Information which identifies parts in a case (the entire table <i>Part in case</i>).</li> </ul>	O
K8.61	It should be possible to screen the following information associated with a registry entry using an access code: <ul style="list-style-type: none"> <li>• Parts of the description of contents (<i>Description of contents</i> in the table <i>Registry entry</i>): The system should either permit the screening of everything but the first part of the description of contents (e.g., the first line) or screening of individual words which the user highlights.</li> <li>• Case part (<i>Case part</i> in the table <i>Registry entry</i>): Used e.g. when a case part is specified using an object code which is a person name.</li> <li>• Information which identifies the sender and/or addressee (the attributes <i>Name</i>, <i>Short name</i>, <i>Address</i>, <i>E-mail address</i>, <i>Reference</i> in the table <i>Sender/Addressee</i>).</li> </ul>	O
K8.62	It should be possible to screen the following information associated with electronic documents using an access code: <ul style="list-style-type: none"> <li>• All information concerning a document in the tables <i>Document description</i> and <i>Version</i> as well as the document itself (the text) is screened together, i.e., it is checked off once. Excepted from screening is the public version of the document, if such a version exists (the attribute <i>Variant</i> in the table <i>Version</i> = O).</li> </ul>	O2
K8.63	It should be possible to screen notes, cfr. the table <i>Note</i> . The screening of a note should include all its information.	O2
K8.64	It should be possible to screen additional information, cfr. the table <i>Additional information</i> . The screening should include all information.	O1
K8.65	It should be possible to screen information on precedent, cfr. the table <i>Precedent</i> . The screening should include all information.	O

When a user registers an access code, the following functionality for the screening of information should be provided:

K8.66	The user should be able to check off what information is to be screened. It should then be possible for the system to show what information is checked off, in all contexts where this is appropriate.	O
K8.67	It should be possible to check off collectively the information to be screened, for instance by using the number codes specified in Noark-3 and Koark.	A

K8.68	When an access code is registered for a case, it should be possible to check off for the screening of information related to the case, cfr. K8.60.	O
K8.69	When there are several parts in a case, it should be possible to screen them individually, but it should also be possible to check them off collectively.	O1
K8.70	When an access code is registered for a registry entry, it should be possible to check off for the screening of information related to the registry entry as well as for electronic documents associated with the registry entry, cfr. K8.61 and K8.62.	O
K8.71	When a registry entry has several senders or addressees, it should be possible to screen these individually, but it should also be possible to check them off collectively.	O1
K8.72	The screening of registered electronic documents should always be carried out from a registry entry with which they are associated. It should be possible to register an access code for the registry entry when the associated documents are to be screened, without having to check off any of the records information for screening, cfr. screening code 1 in Noark-3 and Koark.	O2
K8.73	The electronic main document of a registry entry should always have the same access code and (if applicable) the same access group as the registry entry. The values are inherited when the registry entry is registered or modified, and it should not be possible to modify them in any other way.	O2
K8.74	Electronic documents which are not main documents of a registry entry, should inherit the access code and any access group of the registry entry as default value, unless they have already been assigned an access code or access group and provided they are not already associated with another registry entry. If no access code or access group is inherited when a registry entry is registered or modified, the user should be notified. It should be possible to modify the access code and any access group for documents which are not main documents of a registry entry.	O2
K8.75	Notes (see K8.63) should inherit the access code and any access group from the case, registry entry or document with which they are associated. It should be possible to modify the values.	O2
K8.76	Additional information (see K8.64) should inherit the access code and any access group from the case, registry entry or document with which it is associated. It should be possible to modify the values.	O1
K8.77	Precedents (see K8.65) should inherit the access code and any access group from the case with which they are associated. It should be possible to modify the values.	O
K8.78	Except as specified in K8.73 – K8.77, access codes and access groups should not be inherited from one level to the next (e.g., from case to registry entry).	O
K8.79	Only information which is checked off for screening, should be screened against access by unauthorized users.	O
K8.80	When the user retrieves a case or registry entry, a prompt in the screen panel should indicate whether there are subordinate units which contain screened information. It should be possible to display detailed information according to need, for instance in a separate panel.	O1

#### 8.2.3.4 Temporary blocking of newly registered information

When a new case or document is registered (registry entry, etc.), it is not always clear whether the information should be publicly available or not. This applies in particular to incoming documents (document type I), which are normally registered by the registry office. It is not the task of the registry office to decide what information, if any, should be exempt from public access; this decision usually rests with the manager of the department/section/office or with someone higher up in the hierarchy. Even for documents produced by the organization itself, this matter has not always been decided on when the document is finalized by the executive officer.

In order to prevent sensitive information from becoming known to unauthorized persons before a decision has been made as to its public availability, Noark-4 introduces an automated function for temporarily blocking newly registered information. It is, however, left to the individual organization to decide whether this function is to be implemented or not.

K8.81	The organization should be able to configure a setup whereby all new cases and registry entries (including associated information and documents) which are registered in one or more registry management units, are automatically assigned access code XX, and all information which may be screened using access codes (see K8.60 - K8.65 above) is automatically checked off for screening.	O1
-------	---	----

This will result in the information being unavailable to other persons than those authorized to see them, until the XX code is revoked or replaced with another access code.

The authorization for access code XX follows the usual principles. All users should by default be cleared for access code XX. The authorization should normally be limited to cases for which the person is case-responsible and documents for which he/she is executive officer. If somebody is to have access to information which is blocked using access code XX for which he/she is not executive officer (e.g., registry personnel or certain managers), he must be authorized for this access code in the normal way. Managers should normally be authorized for the administrative unit which they head, and registry personnel for the units for which they register. Beyond this, access is restricted according to record-organizational and/or administrative principles as mentioned in K8.53.

K8.82	The temporary blocking of a registry entry should be revoked using a separate command. This command should remove the XX code (it should not be possible to remove the code in any other way) and provide for the assignment of a new access code if the document is to be exempt from public access. It should be possible to revoke the XX code for individual registry entries. However, there should also be a way of revoking the block collectively for all registry entries having the same record date, possibly with a prompt asking whether separate access codes should be registered for individual registry entries. When the XX code is revoked for a registry entry, it is automatically revoked for all associated information as well as for the latest version of all associated documents.	O1
-------	---	----

K8.83	When the XX access code is revoked, the attribute <i>Public access evaluated</i> (table: <i>Registry entry</i> ) is automatically filled in with the current date.	O1
K8.84	When the XX access code is revoked for the first registry entry of a case, the XX access code is automatically revoked for the case, too.	O1

Fixed procedures must be established for revoking the temporary block, cfr. 8.3.3 below. To support such procedures, the system should provide for the following:

K8.85	The user should be able to search for cases and documents (registry entries) coded XX which are registered prior to a certain date.	O1
K8.86	The system should have an automated reminder function which makes the user aware of blocked cases/documents which are older than a certain number of days. The organization itself should be able to set the exact number of days.	O1

### 8.2.3.5 Public access to information - public registry and access to documents

The principle of public access is inherent in the Freedom of Information Act and implies that the general public should have access to the records information and case documents which are not subject to a special provision exempting them from public access in accordance with §§ 5, 5a and 6 of the Freedom of Information Act, cfr. also the regulation, ch. V no. 7. In this context, the general public is primarily represented by journalists. The principle of public access is practised by having public bodies present public registry, and journalists may on the basis of this registry claim access to the actual case documents.

The access control of Noark-4 is designed with a view to enabling the users to fulfil the requirements of the Freedom of Information Act completely. The principles on which it is based, have been presented to the Legislation Department of the Ministry of Justice, who is administratively responsible for the act.

The relations with the principle of public access mainly concern the layout of the public registry. However, provision is also made for processing requests for access to electronic case documents as well as handling external users who are connecting to the Noark base itself.

K8.87	The public registry should be a standard report (to paper or file) according to the description in chapter 11.	O
K8.88	The public registry may also be an export function (electronic). It should contain the same information as the standard report (ch. 11), and it should follow the export format described in paragraph 15.4.2.	O1
K8.89	The public registry should be available in electronic form, as a function in the system.	A

The information to be included in the public registry is based on the Archives Regulation. This is included in the description of the public registry as standard report (ch. 11).

K8.90	In the public registry, registry entries are displayed in chronological order. Information concerning a case is associated with individual registry entries, cfr. ch. 11.	O
K8.91	A public registry, as a report or electronic export function, may potentially include one or more record dates (the attribute <i>Record date</i> in the table <i>Registry entry</i> ).	O
K8.92	If the function for temporary blocking with access code XX is used, a public registry may potentially include the registry entries whose temporary blocking was revoked on one or more dates (the attribute <i>Public access evaluated</i> ) - see also paragraph 8.3.3 on procedures.	O1
K8.93	Registry entries which are temporarily blocked (access code XX), are excluded from the public registry until the block has been revoked.	O1
K8.94	All registry entries within the dates included in a public registry according to K8.91 or K8.92 which have not been assigned access code XX, should be included in the public registry. Internal documents (types N, X and S) should be handled in the same way as external (types I and U).	O
K8.95	The screening of information in a public registry should be carried out on the basis of access codes according to the following principles: <ul style="list-style-type: none"> <li>• For registry entries which do not have an access code (i.e., the code is blank), all information included in the registry is displayed, cfr. chapter 11.</li> <li>• For registry entries which have access codes, the information which is checked off according to the principles in K8.60 - K8.62 above, is screened. This means, among other things, that parts of the description of contents will always be displayed in the public registry (see also paragraph 8.3.3 below concerning procedures).</li> </ul>	O

*Note: Organizations which resort to temporary blocking using access code XX, should definitely follow the principles in K8.92 and let the public registry include the registry entries whose blocking was revoked on a certain date. This would ensure that all registry entries are included in the public registry, cfr. paragraph 8.3.3 concerning procedures.*

Matters relating to access to case documents should be dealt with by the organization whenever requests for access are received. Even so, it is still permissible, and usually appropriate, to register access codes on electronic documents which contain sensitive information, when the blocking of records information is revoked. This is dealt with in more detail under procedures in paragraph 8.3.3.

As the administration gains experience in electronic recordkeeping and records management, some organizations may want to let external users (journalists and others) search for publicly available information in the Noark base itself. If so, this offer will go beyond what is required by the Freedom of Information Act.

Noark-4 is designed with a view to such opportunities. It is possible to create a separate user type (role) as external user, role 7 - EKS, cfr. K8.9 above. The following particular restrictions apply to read access if a user with role EKS is created:

K8.96	Users having role EKS should only be able to search in and retrieve information which is included in a public registry.	A
K8.97	If the role EKS is defined, there should be a configurable setting which determines whether users with the EKS role may retrieve electronic documents which are not screened, or if retrieval of documents should always require a request for access to information.	A

### 8.2.3.6 Time limits for screening through access codes

It should be possible to use time limits for the individual access codes to indicate the duration of the screening. This should be a support function to limit the screening in time in accordance with the current laws and regulations. The following functionality is required:

K8.98	For each access code, there should be a time limit. The time limit is registered as the date on which the screening should be (re)evaluated or revoked (the attribute <i>Date of downgrading</i> ). If the date field is blank, this means that no time limit has been specified.	O
K8.99	It should be possible to fill in the date straight away, or the date may be calculated by the system when the user specifies the number of years.	O1
K8.100	The predefined access codes in Noark should be associated with regular time limits which the system uses for the automatic registration of a date of downgrading for each registry entry. The date is calculated on the basis of <i>Record date</i> . The following regular time limits apply: <ul style="list-style-type: none"> <li>• Codes according to the safety instruction and the security and protection instruction, i.e., the codes <b>B, K, H, F, SF</b>: 30 years.</li> <li>• Codes which indicate professional secrecy according to § 5a of the Freedom of Information Act, including further specifications, i.e., code <b>5a</b> and specialized codes with this statutory authority: 60 years.</li> <li>• Code for temporary blocking, i.e., code <b>XX</b>: 14 days.</li> <li>• Other codes: blank.</li> </ul>	O

The attribute *Downgrading code* is used to indicate what is going to happen when the specified date is reached. The system should provide functionality for effectuating the downgrading, i.e., revoking the access code based on the downgrading codes.

K8.101	There should be functions for effectuating the downgrading, i.e., revoking the access code for one or more registry entries based on the downgrading code, cfr. the attribute <i>Downgrading code</i> . It should be possible to carry out the downgrading using a particular command, either for individual registry entries or for all registry entries which fulfil the criteria, i.e., their date of downgrading has been reached and their downgrading code is either <b>A</b> or <b>S</b> (cfr. the attribute <i>Denomination</i> in the table <i>Downgrading code</i> ). When a registry entry has been downgraded, the system should automatically set the <i>downgrading code</i> to <b>AU</b> .	O
K8.102	When a registry entry is downgraded, the system should automatically revoke the access code of associated information and of the latest version of associated documents, provided that their access codes are	O1

	identical to that of the registry entry.	
K8.103	When the first registry entry in a case is downgraded, the access code of the entire case should be revoked, provided that it is identical to that of the registry entry.	O
K8.104	In an enhanced version of Noark-4, it should be possible to have the downgrading effectuated automatically when the date of downgrading is reached. This should be done for registry entries whose <i>downgrading code</i> is <b>S</b> , but only if the <i>registry status</i> is <b>J</b> or <b>A</b> . Automatic downgrading should be logged, cfr. the table <i>Additional information</i> .	O1

## 8.3 Procedure requirements

Sub-chapter 8.2 describes how the user management and access control must be designed to satisfy the requirements of Noark-4. The administrative procedures required to make these functions work according to plan are described in the following.

### 8.3.1 User-management procedures

Two kinds of procedures are associated with user management:

- All users, access codes and access groups must be registered in the system. The users must be given rights relating to (authorization for) certain roles, functions in the system and access to information. This is effectuated in one operation when the system is implemented. However, these registrations must be kept up to date. Changes must be made when people quit or are given new tasks, when new people are employed, etc. Changes must also be made when tasks, work routines or the internal organization are modified. It is important that this updating is taken seriously, and that the management considers carefully what roles and rights individuals should have. The quality of the database and the security in connection with the screening of sensitive information depend on this.
- It is necessary to establish procedures which in the best possible way ensure that the individual users maintain their functions in the system according to the intention. This necessitates the establishment and updating of a clearly set-out description of procedures, and the management must follow up the procedures on a regular basis.

### 8.3.2 Procedures for managing write access

More than before, Noark provides for a number of options with regard to the functionality of the system. There is the option of traditional usage (as in Noark-3), but there is also functionality for advanced electronic case handling and recordkeeping based on the executive officers being assigned extensive rights with regard to registration. The system's provision for such advanced usage does not, however, mean that this is appropriate or advisable in all contexts. This will depend very much on maturity and active preparation. For organizations without adequate procedures and organizational skills, such liberal practice with regard to the executive officers' registration rights may be totally

unjustifiable. In other words, Noark-4 results in greater tension between the options offered by the system and the qualifications of the organizations regarding their use. For most organizations, a major challenge will be to evaluate the usage in the light of current and planned organizational structure and procedures.

In organizations of a certain size, the enhanced registration rights for managers and executive officers require a permanently working apparatus to administer and update the user rights. Likewise, an adequate apparatus is required for follow-up and quality control (registry office). In addition, there is a need for clearly defined and authoritative procedures and executive officers who are well versed in these procedures. It may be sensible to start by introducing electronic case handling with its enhanced registration rights for managers and executive officers in one, or a small selection of, unit(s) within an organization. This allows for concentration, both with regard to training and follow-up of users, and such a scenario with pilot users also makes it easier to gain valuable experience with new procedures.

Neither should the option of having differentiated rights for executive officers on a more permanent basis be ruled out completely. For various reasons, there will always be executive officers with variable training and qualifications for the correct use of the recordkeeping system.

### **8.3.3 Procedures for managing read access**

#### **8.3.3.1 General**

In line with the above discussion, the following must be registered before the system can be implemented and changes made to update it:

- any restrictions in the individual users' access to information based on administrative and/or record-organizational criteria (see 8.2.3.1 above)
- access codes used by the organization
- statutory authorities for these access codes (Freedom of Information Act, any additional statutory authority for professional secrecy, etc.)
- clearance of individual users for access codes as well as their authorization for the information screened with these codes
- any fixed access groups
- any members of fixed access groups

Furthermore, a description of what the individual access codes and access groups mean and are to be used for, must be prepared and kept up to date. This material should be easily available to those who use the system, particularly those who perform registration tasks.

#### **8.3.3.2 Revoking temporary blocking**

Regular procedures must be established with regard to how the blocking of newly registered cases and case documents/registry entries are revoked. These procedures should, on the one hand, ensure that only authorized persons may revoke the blocking, on the other hand it should ensure that the blocking is not maintained for longer than necessary. The following must be made clear:

- Who is to decide on public access or screening in the individual cases

- Who is authorized to revoke the blocking (authorization in the Noark system)
- Procedures which ensure that the question of public access/screening is dealt with within a reasonable period of time (note that the default time limit for blocking set by the system is 14 days)
- Procedures for communicating between those who make the decision and those who revoke the blocking (if these are different persons)
- Time limit for automated reminder that the blocking has not been revoked, if the system has this function (see 8.2.3.4 above)

### 8.3.3.3 Producing public registry

Procedures must be established for the printing of public registry, and for the content of the daily version of this registry. It is recommended that one of the following procedures be followed (cfr. the functions for public registry in 8.2.3.5 above):

- If information is temporarily blocked (see 8.2.3.4 above), the public registry is printed at the beginning of the working day and includes all registry entries which were evaluated with a view to public access the day before, i.e., the attribute *Public access evaluated* is filled in with the date of the previous day.
- If temporary blocking of information is not practised, the public registry should include all registry entries which were registered on the same day (e.g., the day before printout), i.e., all that have the same value in the attribute *Record date*.

This should ensure that all registry entries are included in the public registry, and that none of them are included twice.

When parts of the title field on a case or parts of the description of contents on a registry entry are screened (see 8.2.3.3), it is necessary to make sure that the part of the text which is public (available), makes sense without giving away the information to be screened.

### 8.3.3.4 Processing requests for access to case documents

When requests for access to case documents are forwarded by journalists or other members of the public, the organization must decide on the question of public access on receiving the request. Nevertheless, it will often be necessary to evaluate a case document in relation to the exemption provisions of the Freedom of Information Act even when no request for access to the document has been forwarded. During registration, there will thus be a need for pre-evaluation of the document in order to prevent information which must or should be exempt from public access, from being made known to unauthorized persons at the time of entry into records. This applies in particular to information subject to professional secrecy (§ 5a of the Freedom of Information Act).

The following procedures are recommended in connection with Noark-4:

- Documents which are publicly available, are not assigned an access code in the system. This means the documents may, without further ado, be presented or copied to journalists and other members of the public on request. It also means that such documents in electronic form are openly available to all internal users in the system (possibly excluding some based on administrative or record-organizational criteria, as discussed above).

- Documents which have been evaluated or are to be evaluated with a view to exempting them from public access, are assigned an access code in the system. For such documents, decisions concerning access are made individually when requests for access are received (see, however, the next indent). When such documents are stored electronically, they will also be screened against internal users who are not authorized for the concerned code.
- In line with the opportunities provided by the system, the organization may, in situations where requests for access to a document are likely to appear, consider storing a "public" version of the document where information which is exempt from public access, is left out. The "public" version of the document must then be without an access code, whereas the original version is screened. "Public" document versions which are stored electronically, are identified through a separate version type in the system (see paragraph 5.2.4 above).

### 8.3.3.5 Registering time limits for screening - revoking access codes, downgrading

It is recommended that default time limits be defined for all access codes for which this is practicable, and that a time limit be defined where blank when cases and registry entries/documents are registered. During registration, it ought to be considered whether screening should apply for a shorter period of time than that of the default value (this does not apply to screening due to professional secrecy according to § 5a of the Freedom of Information Act).

Public bodies should establish regular procedures for revoking access codes when the time limit is reached. This can be done easily by searching periodically for registry entries for which the time limit has expired (see the report in 11.3.6 below), and, if justified, revoking the access code for the registry entry and, if applicable, for its associated case information and case documents.

## 8.4 Essential tables in the module

Only essential tables have been included here. For a complete overview of the tables in the module and their attributes, see part II, Technical specifications, sub-chapter 14.5.

Table name	Text
Person	Contains all persons in the organization who have rights in the system, as well as all persons to whom the system refers (executive officer, board member, etc.) The identification used for logging on to the system is also stored here.
Person name	Contains the full name of the person as well as his/her official initials as used for registration purposes. A person may be associated with several person names. A separate flag indicates whether this is the person's current name and initials. This is a way to store the history associated with change of name, etc.
Role	Contains information on the rights inherent in a specific role.
Person - role	Associates a person with a specific role. A person may have several

Table name	Text
	roles, one of which must be his/her default role (basic role). The table also associates the person with an administrative unit, registry management unit and records section.
Access code	Contains the access codes which the system uses. Most of the codes are predefined, but it is also permissible to create customized codes.
Clearance for access code	Contains information on the access codes for which a person is cleared. The table has a link to the administrative unit.
Statutory authority for access code	Statutory authority for information exempted from public access, linked to access code.
Access group	Used to store the names of the defined access groups. Access groups are used to limit the access further among the users who are authorized for a specific access code.
Membership in access group	Contains information on the access groups which a person in a specific role is member of.

## 8.5 Changes from Noark-3 and Koark

The user management and access control is extended and made more flexible than in Noark-3 and Koark. Chapter 16 contains a complete technical specification of the changes and how conversions may be carried out. The most important changes are summarized here:

### Basic version (requirement type O):

- The user types have been replaced with roles in Noark-4. Rights and restrictions are associated with the individual roles.
- A person may be registered under several names and initials, and be associated with several roles. This is new.
- The concept of *access code* (attribute) replaces that of *grading code*, cfr. chapter 4.
- A user is (generally) *cleared* for an access code and *authorized* for the code within specific parts of the base. This use of concepts represents a slight change from Noark-3 and Koark.
- Access codes are normally not inherited from one level to another, whereas grading codes normally could be in Noark-3 and Koark.
- A stricter system has been established for indicating the statutory authority of access codes.
- Adjustments have been made as to what information may be screened from public access.
- Screening is carried out by checking off instead of using codes.
- The public registry is more formalized, after a thorough revision (see also chapter 11).

### Enhanced version (requirement type O1):

- Rights and restrictions may also be associated with different stages of the handling process, governed by status values in the records management module.

- In addition to the use of access codes, screening may be effectuated through the use of access groups and according to administrative and/or record-organizational criteria.
- An access code for temporarily blocking information which has not been evaluated with regard to public access, has been introduced.
- The downgrading functions have been made more flexible.