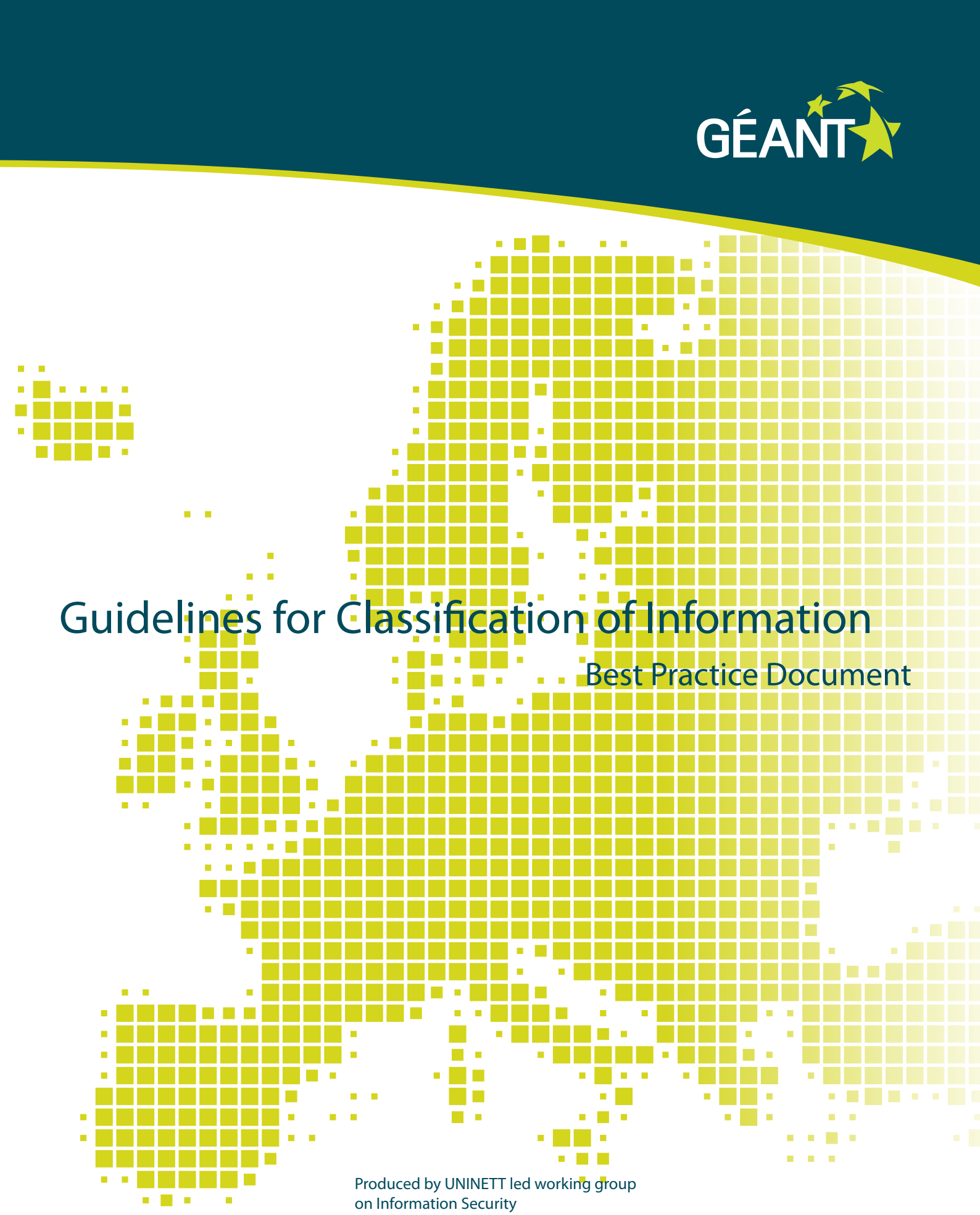

Guidelines for Classification of Information

Best Practice Document

Produced by UNINETT led working group
on Information Security
(UFS 136)

Author: Øivind Høiem

March 2013

Document No: GN3-NA3-T4-UFS136
Version / date: 2013-03-18
Original language: Norwegian
Original title: “Retningslinjer for klassifisering av informasjon ”
Original version / date: 1.0 of 2013-03-18
Contact: campus@uninett.no

UNINETT bears responsibility for the content of this document. The work has been carried out by a UNINETT led working group on Information Security as part of a joint-venture project within the HE sector in Norway.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 238875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Executive Summary		4
1	Introduction	5
2	Classification of information	6
Appendix 1: Proposed information classification		9
Appendix 2: Archiving		14
Appendix 3: Preservation and destruction schedule		15
Appendix 4: Unrestricted data in the public sector		16
Attachment 5: Standards, laws and regulations		18
References		22
Glossary		23

Executive Summary

This document specifies the recommended guidelines for information classification in the higher education institutions in Norway. Means of identifying and in turn classifying the institution's information objects are given. Classification is done based on sensitivity and criticality. Adequate retention periods and disposal regulations are suggested. Careful measures should be taken before approving storage of information objects on mobile devices and cloud-based services.

The guidelines include examples of how information objects which are frequently used in the Higher Education sector can be classified, as well as references to relevant standards, laws and regulations.

The guidelines will serve as an important tool set for information owners to secure mission-critical content.

1 Introduction

The purpose of these guidelines is to describe how one can identify information objects in an organisation and classify them with respect to sensitivity and criticality, and to define storage periods and rules for disposal.

This document is also intended to be a tool for information owners to ensure that content which is critical to operations will be taken care of, handled and disposed of in accordance with internal and external requirements and best practice. It is also important to carry out this type of classification before uploading information to a cloud service and when using mobile units such as tablets and smartphones.

Chapter 2 gives an overview of the information classification process and elaborate on the attributes that should be evaluated. Attachment 1 provides examples of how information objects frequently used in the higher education (HE) sector can be classified.

Appendix 2 explains the distinction between an archive, a library and a collection as defined in the Norwegian archive standard (Noark).

A preservation and destruction schedule is important for the operation of an efficient information handling system. It should provide guidelines for the storage and disposal of information generated during day-to-day operations, ensuring continuity, protecting the organisation's legal rights and facilitating the retrieval of the information when needed. See Attachment 3 for further information.

Attachment 4 to the guidelines describes how unrestricted data in the public sector should be made accessible.

Attachment 5 provides an overview of standards, laws and regulations which the institutions must take into account in connection with classification work. Links to further information is given.

Some of the classifications, such as security classification, security requirements, maximum downtime and preservation value, should be based on a risk and vulnerability (RAV) assessment and/or a Business Impact Assessment (BIA). The guidelines have been prepared by the information security secretariat in UNINETT in collaboration with the HE sector.

The document contains several references to Norwegian laws and regulations. Unfortunately most of the references are only available in Norwegian. We have chosen to keep the Norwegian references as it is beyond the scope of this document to find the EU equivalents, if they exist.

2 Classification of information

The Classification of information may be carried out using the table below. A description of the columns follow and an example is given in appendix 1.

Owner	Content	Legal authority	Storage location	Unrestricted data? (Open)	Security classific-ation	Security require-ment	Max. down-time	Preserv-ation value	Personal data? (P/S)	Archive index	Storage period	Disposal

Description of columns

Owner
The organisational unit or process which holds ownership of the information.

Content
Type of information, irrespective of format and medium. What the information applies to.

Legal authority
Reference to a regulatory document (law, rule, regulation, governing document) which specifies storage and/or disposal requirements. For example, Chapter 25 of Norwegian Act No. 16 of 19 May 2006 relating to the right of access to documents held by public authorities and public undertakings (the Freedom of Information Act) or Section 13.1 of the Act of 10 February 1967 relating to procedure in cases concerning the public administration (the Public Administration Act).

Storage location
The name of the system (e.g. Noark system, other electronic journal, management system, financial system, etc.) and/or physical archive in which the information object is located in the storage period.

Unrestricted data?
The Norwegian Ministry of Government Administration, Reform and Church Affairs (FAD) and the Agency for Public Management and eGovernment (Difi) wish to make it possible for public enterprises to share their data so that they can be used in new contexts and in providing new services. To ensure that data are made available in a practical manner, public enterprises should follow FAD's guidelines. See Attachment 4 "Unrestricted data in the public sector" for more information.

Security classification
The degree of protection required for the information object. If the information, e.g. incoming mail, can have more than one level of classification the word "**Variable**" shall be written in this field.

Classification level:

- **Open** information may be accessible by both external parties and the enterprise's employees without special access rights.
- **Internal** information may be accessible by both external parties and the enterprise's employees with controlled access rights.
- **Confidential** information will normally only be accessible by employees with strictly controlled access rights. In special cases, Confidential information may also be made accessible to external parties assigned strictly controlled access rights, for example personal data for which permission has been granted for communication to others.

Security requirement
Here one takes into consideration special security requirements based on the confidentiality, integrity and/or accessibility of information objects.

- **C** – The information object contains sensitive information and shall be handled **confidentially**
- **I** – The **integrity** of the information object shall be specially protected against unintentional or conscious unauthorised changes
- **A** – The information object shall be handled especially with regard to high **accessibility**

Maximum down-time
The maximum acceptable time for which electronically stored information can be inaccessible. For some systems, the acceptable down-time may vary throughout the year in consideration of, for example, examinations, admissions, reporting, etc. Recommended periods are:

- **1 HOUR**
- **1 DAY**
- **1 WEEK**
- **1 MONTH**

Preservation value
Preservation value is a criterion which specifies the relative importance the information has for the organisation.

- **LEG** – Legal value
- **ENT** – Enterprise-critical value
- **HIST** – Historical value

Personal data
If the information object contains or may contain personal data, this should be indicated in the table.

- **PERSONAL DATA (P)** are data and judgments which can be associated with a private individual.

- **SENSITIVE PERSONAL DATA (S)** may be information relating to racial or ethnic background, political, philosophical or religious persuasion, state of health, sexual preference or membership of organisations. It may also indicate whether a person has been suspected, charged, prosecuted or convicted of a punishable offence.

Archive index
An archive index is a system for organising case files based on one or more classification principles. Archive indices describe principles of classification and sorting systems and normally use a sorting principle based on subjects. According to the Norwegian Archives Regulation, government agencies shall use the "Common

Archive Index for Public Administration". A common archive index has been created for state-run colleges, which also includes a data destruction schedule.

The subject groups, and thereby the folders in the physical archive, are organised according to the decimal system. The principle of this system is that subject areas are divided into up to ten groups which are assigned numbers 0 to 9. Each of these groups is then divided into ten new sub-groups, deriving from and bound to the subject area above. Each of these may in turn be divided into ten sub-groups, and so on. The highest level in the hierarchy is called a class.

Examples:
Class 1 is Finance
Main Group 13 is Accounting and Auditing
Group 133 is Completed Accounts

Storage period
The period for which information shall be stored in the archive. The storage period commences when an information object is created and is specified in years.

- **PERMANENT (PERM)** – the information object shall be stored permanently.
- **LIFETIME-RELATED (LT)** – the information object is lifetime-related in relation to other objects (computer systems, projects, programmes, contracts, buildings, employment terms, study terms, etc.). It is common to specify a storage period of 5 or 10 years after completion of a project, termination of a contract, etc.
- **nn YEARS** – the enterprise has defined the storage period, for example if the storage period is connected with an incident or activity or is imposed by legislation.

Disposal rules
Rules governing the disposal of information at the end of the storage period. Note that there may be special rules for the storage of information which applies to one's own activities or which are of fundamental nature. Routine individual matters which are no longer of administrative significance may often be destroyed.

- **REVIEW (REV)** – send the information object to the information owner for review at the end of the storage period.
- **DESTROY** – destroy the information object immediately at the end of the storage period. Note that information objects which contain personal data require secure destruction.
- **DEPOSIT** – deposit the information object in the archive depot at the National Archives at the end of the storage period.
- **KEEP** – not to be disposed of because of requirement for permanent storage.

Appendix 1: Proposed information classification

The following is a proposal for information classification for individual information objects used in the higher education sector in Norway. Classification of information objects is based on a study of the sector, but does not include all the types of objects used there. The table is intended to be a starting point and must be reviewed and edited by each individual enterprise. This is particularly important with regard to storage location, storage period and disposal rules. Storage location, maximum downtimes and archive indexes may also be specified in the table. Data destruction schedules should be created on the basis of the enterprise's archive index.

Owner	Contents	Legal authority	Storage location	Unre-stricted data? (Open/ N)	Security classification	Security require-ment	Max. down-time	Preserv-ation value	Person-al data? (P/S)	Archve index	Storage period	Disposal
R&D	Research project I	Freedom of Information Act S. 26.4		Open	Internal	(C)IA		ENT, HIST	-		LT	REV
R&D	R&D applications	Freedom of Information Act S. 26.4		N	Internal	CIA		-	P-		LT	REV
R&D	R&D allocations			Open	Open	I		ENT	-		LT	REV
R&D	Contracts			N	Internal	CIA		ENT, LEG	(P)		LT	REV
PERS	HSE management			Open	Open	I		-	-		LT	DESTROY
PERS	Employment agreements	Freedom of Information Act S. 25.1, Public Administrati on Act S. 13.1		N	Internal	CI		LEG	S		LT	DESTROY
PERS	Working environment initiatives (individual)	Freedom of Information Act Ch. 13, Public Administrati on Act S. 13.1		N	Internal	CI		-	S		LT	DESTROY
PERS	Working environment initiatives (group)	Freedom of Information Act Ch. 13, S. 23.1, Public Administrati on Act S.		N	Internal	(C)I		-	S		LT	DESTROY

Owner	Contents	Legal authority	Storage location	Unre-stricted data? (Open/ N)	Security classification	Security require-ment	Max. down-time	Preserv-ation value	Person-al data? (P/S)	Archve index	Storage period	Disposal
		13.1										
PERS	Disciplinary matters	Freedom of Information Act Ch. 13, Public Administrati on Act S. 13.1		N	Confidential	CI		LEG	S		LT	DESTROY
PERS	Union negotiations	Freedom of Information Act Ch. 14, S. 23.1		N	Internal	(C)IA		-	P		LT	DESTROY
PERS	Union negotiations – minutes			Open	Open	I		LEG	P		LT	REV
PERS	Equal opportunity work			Open	Open	I		-	-		LT	DESTROY
PERS	Salary and personnel data	Freedom of Information Act S. 13.1, cf. Public Administrati on Act Ch. §13		N	Internal	CIA		ENT, LEG	P(S)		LT	DESTROY
PERS	Salary negotiations	Freedom of Information Act S. 23.1		Open	Internal	CI		ENT, LEG	P		LT	DESTROY
PERS	Salary negotiations (individual)			N	Internal	CI		LEG	P(S)		LT	DESTROY
PERS	Employee appraisal interviews	Freedom of Information Act Ch. 13, Public Administrati on Act S. 13.1 Not in archive		N	Confidential	CI		LEG	P(S)		LT	DESTROY
PERS	Reorganisation – process	Freedom of Information Act Ch. 14, S. 23.1, Public Administrati on Act S. 18a		N	Internal	CI		-	P(S)		LT	REV
PERS	Reorganisation – result			Open	Open	I		ENT	P		LT	REV
PERS	Sickness follow-up	Freedom of Information Act Ch. 13, Public Administrati on Act S. 13.1		N	Internal	CI(A)		-	S		LT	DESTROY
PERS	Promotion	Freedom of Information Act S. 23.1, S. 25.1		Open	Internal	(C)IA		-	P		LT	DESTROY
PERS	Leave of absence	Freedom of Information Act Ch. 13,		N	Internal	CI		-	P(S)		LT	DESTROY

Owner	Contents	Legal authority	Storage location	Unre-stricted data? (Open/ N)	Security classification	Security require-ment	Max. down-time	Preserv-ation value	Person-al data? (P/S)	Archve index	Storage period	Disposal
		Public Administrati on Act S. 13.1										
PERS	Minutes of negotiations			Open	Open	I		LEG, ENT, HIST	P		LT	REV
PERS	Scholarships			N	Internal	I		-	P		LT	DESTROY
PERS	Statements of Confidentiality			N	Open	I		LEG	P		LT	DESTROY
PERS	Employment	Freedom of Information Act Ch. 25		Open	Open	I(A)		-	P		LT	DESTROY
PERS	Employment recommendations	Freedom of Information Act Ch. 25, Public Administrati on Act S. 13.1		N	Internal	CI		-	P		LT	DESTROY
PERS	Employment applications	Freedom of Information Act Ch. 25, Public Administrati on Act S. 13.1		N	Internal	-		-	P		LT	DESTROY
PERS	Notification issues	Freedom of Information Act Ch. 13, Public Administrati on Act S. 13.1		N	Confidential	CI		LEG	S		LT	DESTROY
STUD ADMIN	Deviation notifications			N	Confidential	CI		LEG	P(S)		LT	DESTROY
STUD ADMIN	Deviation notifications, study progression	Freedom of Information Act S. 13.1, cf. Public Administrati on Act Ch. §13		N	Internal	CIA		LEG	P(S)		LT	DESTROY
STUD ADMIN	Exam papers	Before exam: Freedom of Information Act S. 26.1		N	Confidential. Open after exam completed	CIA		ENT, HIST			PERM	KEEP
STUD ADMIN	Change of personal ID number			N	Internal	CI		-	P		LT	DESTROY
STUD ADMIN	Curricula			Open	Open	IA		ENT, HIST	-		PERM	KEEP
STUD ADMIN	Applications for exemption	Freedom of Information Act Ch. 13, Public Administrati on Act S. 13.1		N	Internal	CI		-	P(S)		LT	DESTROY
STUD ADMIN	Cheating issues	Freedom of Information Act Ch. 13, Public Administrati		N	Confidential	CI		LEG	S		LT	DESTROY

Owner	Contents	Legal authority	Storage location	Unre-stricted data? (Open/ N)	Security classification	Security require-ment	Max. down-time	Preserv-ation value	Person-al data? (P/S)	Archve index	Storage period	Disposal
		on Act S. 13.1										
STUD ADMIN	Visitor and private candidate applications			N	Internal	CI		-	P(S)		LT	DESTROY
STUD ADMIN	Incorporation of subjects	Freedom of Information Act Ch. 13, Public Administration Act Ch. 13		N	Internal	CI		-	P(S)		LT	DESTROY
STUD ADMIN	Internationalisation	Freedom of Information Act S. 13.1, cf. Public Administration Act Ch. §13		N	Internal	(C)IA		-	P(S)		LT	DESTROY
STUD ADMIN	Complaints	Freedom of Information Act Ch. 13, Public Administration Act S. 13.1		N	Internal	CI		LEG	P(S)		LT	DESTROY
STUD ADMIN	Loan issues (foreign students)	Freedom of Information Act S. 13.1, cf. Public Administration Act Ch. §13		N	Internal	(C)IA		-	P(S)		LT	DESTROY
STUD ADMIN	Masters' and PhD theses			Open(Unless by except.)	Open	IA		HIST			PERM	KEEP
STUD ADMIN	Admissions	Freedom of Information Act S. 13.1, cf. Public Administration Act Ch. §13		N	Internal	(C)IA		ENT	P(S)		LT	DESTROY
STUD ADMIN	Transfers and course changes	Freedom of Information Act Ch. 13, Public Administration Act S. 13.1		N	Internal	CI		-	P(S)		LT	DESTROY
STUD ADMIN	Leave of absence	Freedom of Information Act Ch. 13, Public Administration Act S. 13.1		N	Internal	CI		-	P(S)		LT	DESTROY
STUDADMIN	Examiner lists			Open	Open	IA		LEG			PERM	KEEP
STUD ADMIN	Invigilating and exam handling	Freedom of Information Act Ch. 26.3		N	Confidential	CIA		LEG	P		LT	DESTROY

Owner	Contents	Legal authority	Storage location	Unre-stricted data? (Open/ N)	Security classification	Security require-ment	Max. down-time	Preserv-ation value	Person-al data? (P/S)	Archve index	Storage period	Disposal
STUD ADMIN	Suitability issues	Freedom of Information Act Ch. 13, Public Administrati on Act S. 13.1		N	Confidential	CI		LEG	S		LT	DESTROY
STUD ADMIN	Curricula (institution)			Open	Open	IA		ENT, HIST	-		PERM	KEEP
STUD ADMIN	Tutoring	Freedom of Information Act Ch. 13, Public Administrati on Act Ch. 13		N	Internal	CI		-	P(S)		LT	DESTROY
STUD ADMIN	Organisation	Freedom of Information Act Ch. 13, Public Administrati on Act S. 13.1		N	Internal	CI		-	S		LT	DESTROY
STUD ADMIN	Certificates	Section 26.3		N	Internal	(C)IA		HIST	P		PERM	KEEP
BOARD S, COUN CILS AND COMMI TTEES	Convening meetings	Freedom of Information Act Ch. 13, Public Administrati on Act Ch. 13		Open	Internal	CIA		-	P		LT	DESTROY
BOARD S, COUN CILS AND COMMI TTEES	Minutes of meetings	Freedom of Information Act Ch. 13, Public Administrati on Act Ch. 13		Open	Internal	(C)IA		ENT, HIST, LEG	P(S)		PERM	KEEP
ECON	Tenders and procurements	Freedom of Information Act S. 23.3, cf. Public Administrati on Act S. 13.1, ss 2		Open	Internal	CIA		ENT, LEG	-		LT	REV
ECON	Agreements and contracts	Freedom of Information Act S. 23.1		Open	Internal	CIA		ENT, LEG, HIST	-		LT	REV
ECON	Budgets and allocations	Freedom of Information Act S. 23.1		Open/N	Internal	CIA		ENT	-		LT	REV
ECON	Internal control			Open/N	Variable	CIA		ENT	-		LT	REV
ECON	Projects			Open/N	Variable	CIA		ENT	-		LT	REV
ECON	Reports and plans			Open	Open	I		ENT, HIST	-		LT	REV
ECON	Accounting reports			Open	Open	I		LEG, HIST	-		10 years	DESTROY
ECON	Allocation of funds			Open	Open	I		ENT	-		LT	DESTROY
ECON	Financial regulations			Open	Open	I		-	-		LT	DESTROY
ECON	Annual reports			Open	Open	I		HIST	-		PERM	KEEP

Appendix 2: Archiving

The distinction between archive, library and (document) collection can be explained as follows:

An **archive** consists of letters or documents which have been created as part of a company's or government agency's operations. Archive documents are often grouped under cases and are not duplicated to a significant degree, often consisting of unique documents, although circulars and other duplicated documents may also be included in an archive.

A **library** consists of a collection of duplicated documents such as books and periodicals.

A **collection** may often consist of unique documents, but these have been categorised based on a different perspective from one of documenting a process or business matter. For example, a collection of letters received from a (known) person over many years would not normally be called an archive if they were collected afterwards.

Private individuals, companies and government agencies all use archives to varying degrees. Government agencies are obliged by law to keep an archive which satisfies certain rules in order to document their activities.

Noark
Noark is an abbreviation of **Norsk arkivstandard** (Norwegian archive standard). Noark was developed in 1984 as a specification for electronic journal systems in public administration by the Norwegian Directorate of Rationalisation (later Statskonsult) in collaboration with the National Archives, and rapidly established itself as the *de facto* standard.

The currently applicable standard is Noark 5. Revisions of the standard have partly consisted of modernisation in step with technological development and partly of expansion of the information content and functionality of the systems.

Noark is both a joint standard for public administration and a facility for increasing interaction between systems and organisations. A retrieval abstract created according to the Noark 5 standard is suitable for long-term storage. Private enterprises will also find Noark useful.

Section 2-9 of the Norwegian Archives Regulation states that government agencies shall use a Noark-approved system for electronic records and archiving.

Appendix 3: Preservation and destruction schedule

The principal aim in carrying out archive limitation[1] and destruction is to reduce the size of paper archives while also structuring and organising information in electronic archives, while ensuring that archived material with lasting value is preserved for posterity.

The need for destruction arises primarily for economic reasons. Other considerations which necessitate the imposition of time limits on the storage of archived materials are:

- It must be possible to document private individuals' needs and legal rights
- The enterprise's own requirements as regards precedence and uniform handling of cases, and the need for documentation of ownership, financial and legal rights
- Adequate and representative source material must be maintained for use in research activities.

Preparation of proposals for preservation and destruction rules
Section 3-21 of the Archives Regulation places an obligation on government agencies to prepare proposals for data destruction rules within their own operations. This means that the agency shall create an overview of the types of archive material which shall be preserved and destroyed. Such an overview is often referred to as a preservation and destruction schedule because it will also contain deadlines for destruction which are to be adhered to.

Preservation and destruction schedule or simple destruction application?
If an organisation wishes to destroy a single series or assess the preservation and destruction of a single system, it is sufficient to submit a destruction application. The National Archives should therefore be contacted for advice on the most appropriate action in each case.

What should a preservation and destruction schedule contain?
A preservation and destruction schedule should contain:

- A thorough systematic examination and description of the areas of responsibility, functions and existing archives of the administrative agency, department or sector.
- A preservation and destruction assessment consisting of consideration of which archives shall be preserved and which shall be destroyed, as well as the reasons for preserving or destroying them.
- Destruction deadlines.

For further information, see the National Archives' website http://www.arkivverket.no/

[1] "Archive limitation" means that one does not register or archive material which is without value for later case treatment or documentation.

Appendix 4: Unrestricted data in the public sector

The Norwegian Ministry of Government Administration, Reform and Church Affairs (FAD) and the Agency for Public Management and eGovernment (Difi) wish to make it possible for public enterprises to share their data so that they can be used in new contexts and in providing new services. Accessibility and continued use of public data entails allowing trade and industry, research and society in general to obtain access to and make use of information owned by public administration.

The term “public data” refers to all types of information produced or acquired by public enterprises. Public data consist principally of information which is, or can be, digitised and stored electronically. Public data may include business registers, survey data, organisational models, budgets, annual accounts, and so on. When data are made accessible in a machine-readable format, other users will be able to find new ways of using the data, thereby increasing the usefulness of data produced by public administration. Moreover, public administration will become more open and legitimate while interaction in the public sector will be enhanced.

Making data accessible for further use entails in many cases more than simply publishing information so that it can be referenced on a web page. Further use also means making raw data accessible in what are known as “machine-readable formats”, so that computers may be used to interpret and analyse the material. Raw data are data which can be processed by computers, divided up, combined with other data and used in new contexts.

Difi’s guidelines
Difi’s guidelines provide an introduction to how public data can be made available for further use, and contain, among other things:

- Examples of what open data can be used for
- Arguments regarding how public enterprises should share their data
- Practical advice for achieving this.

More information at: http://data.norge.no/blogg/2012/05/veileder-i-tilgjengeliggj%C3%B8ring-av-offentlige-data

FAD’s guidelines for making public data accessible
To ensure that data are made accessible in a practical manner, public enterprises should follow FAD’s guidelines, which deal with:

- The principle of access free of charge
- Machine-readable formats
- Processing
- Documentation
- Copyright
- Visibility
- Feedback

- Permanent addressing.

The guidelines are described at:
http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2012/retningslinjer-ved-tilgjengeliggjoring-a.html?id=708912

Digitising circular P-10/2012
This circular provides guidelines for how enterprises shall digitise in order to achieve better services and enhanced operational efficiency. It contains important instructions and recommendations from various sets of regulations and central government decisions, to provide clarification for the enterprises. The circular also explains the process of ICT-related investments in the 2014 budget.

http://www.regjeringen.no/nb/dep/fad/dok/rundskriv/2012/digitaliseringsrundskrivet.html?id=706462

NLOD – Norwegian Licence for Open Government Data
The Ministry of Government Administration, Reform and Church Affairs (FAD) has prepared a licence agreement which public enterprises may use when making data accessible. When data are licensed under the Norwegian Licence for Open Government Data (NLOD), they may be freely used, subject to certain conditions:

The licence permits:
- copying and distribution
- modifying and/or combining with other data sets
- copying and distribution of a modified or composite version
- using data sets for commercial purposes.

Subject to the following conditions:
- that the licence provider is identified as requested by the licence provider, but not in a way which implies that the licence provider has approved or recommends the user or the user's treatment of the data set
- that the data are not used in a misleading way and are not distorted or incorrectly presented.

On the understanding that:
- data which contain personal data and are subject to confidentiality are not covered by this licence and cannot be used
- the licence provider disclaims all responsibility for the quality of the information and for what the information is used for.

The Norwegian Licence for Open Government Data (NLOD) is published in both Norwegian and English. Further information in English can be found at http://data.norge.no/nlod/en

The data hotel at data.norge.no
Data.norge.no is a register of open data in Norway, and also offers a data hotel for enterprises wishing to use Difi's technical infrastructure to publish their own data in machine-readable formats. See http://data.norge.no

Open Knowledge Foundation
The Norwegian guidelines are based on work done by the Open Knowledge Foundation. Read more about the Open Knowledge Foundation and some of their resources:

- Open Knowledge Foundation: okfn.org
- Open Data Handbook: opendatahandbook.org
- Creative Commons License: creativecommons.org

Attachment 5: Standards, laws and regulations

This appendix gives an overview of relevant Norwegian standards, laws and regulations.

Noark 5 - Norwegian archive standard
http://www.arkivverket.no/arkivverket/Offentlig-forvaltning/Noark/Noark-5/Standarden

See the description in Attachment 1 “Archiving”.

Archive plan and data destruction schedule for state-run colleges
www.khio.no/intranett/filestore/arkivnokkel_kassasjonsplan.doc
This plan is accessible (in Norwegian) on the websites of several institutions, but one location is specified here for the sake of simplicity.

The archive plan dates from 1994. The data destruction schedule was added in May 2001 and was last revised in 2005. A new version of both documents will be prepared in 2013.

The Archive Act
Act No. 126 of 4 December 1992 relating to archives (in Norwegian)
http://www.lovdata.no/all/nl-19921204-126.html

The Archives Regulation
Regulation No. 1566 of 1 December 1991 relating to detailed technical and archiving rules in the use of public archives (in Norwegian)
http://www.lovdata.no/for/sf/ku/xu-19991201-1566.html.

The public administration archiving function has for a considerable time been governed by a special regulatory system. The regulations arose as a result of the need for further stipulation, among other things to govern electronic storage of archive material. In combination the Archive Act and Archives Regulation constitute the core of the regulatory system governing the handling of public archives.

The Archive Act provides a number of general and fundamental rules relating to archives, particularly those in public administration. These rules apply, with few exceptions (cf. Chapter 5 of the Archive Act) to all activities taking place in public administration.

The purpose of the Archive Act is to safeguard archives which have significant cultural or research-related value or which contain legal or important administrative information, so that these can be preserved and made accessible to posterity, cf. Chapter 1 of the Archive Act. Chapter 6 of the Archive Act also stipulates that government agencies have a duty to maintain archives, and that these shall be arranged and organised so that the documents are preserved as information sources for the present and in future.

In combination with the detailed regulations, the Act represents a general legal framework for archive-related issues in public administration, from the time a document is created as part of daily business, through archive limitation and delivery of preservation-worthy archive material to an archive depot, to storage and accessibility for posterity.

The Public Administration Act
Act of 10 February 1967 relating to procedure in cases concerning the public administration (in Norwegian)
http://www.lovdata.no/all/hl-19670210-000.html

This Act governs certain types of archive material by stipulating the rules applying to case handling and the rights afforded to individuals by the Public Administration Act. The purpose of the Act is to govern the rights of citizens when they are in contact with government agencies. The Norwegian Public Administration Act is intended to provide legal safeguards to citizens and to ensure satisfactory case handling. It is a general act which is to be used in all case handling in the absence of any other applicable special legislation.

The Freedom of Information Act
Act No. 16 of 19 May 2006 relating to the right of access to documents held by public authorities and public undertakings (in Norwegian)
http://www.lovdata.no/all/hl-20060519-016.html

The purpose of this Act is to facilitate openness and transparency in public undertakings, thereby enhancing freedom of information and speech, democratic participation, the legal safeguarding of the individual, confidence in the public administration and the influence of the public. The Act shall also facilitate the extended use of public information.

The Legal Deposit Act
Act No. 32 of 9 June 1989 relating to the legal deposit of generally available documents (in Norwegian)
http://www.lovdata.no/all/hl-19890609-032.html

The purpose of this Act is to ensure the deposit of documents containing publicly accessible information in national collections, so that these testimonies to Norwegian culture and society can be preserved and made accessible as source material for research and documentation.

The Personal Data Act
Act No. 31 of 14 April 2000 relating to the processing of personal data (in Norwegian)
http://www.lovdata.no/all/hl-20000414-031.html

This Act governs the processing of personal data using electronic tools and manual processing of personal data involving the creation of a personal register.

The purpose of this Act is to protect individuals against infringement of their privacy through the treatment of personal data. The Act shall contribute to the processing of personal data in accordance with basic personal privacy considerations. It shall also take into account the need for personal integrity, privacy and adequate quality of personal data.

The E-administration Regulations
Regulation No. 988 of 25 June 2004 relating to electronic communication with and within public administration (in Norwegian)
http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20040625-0988.html

The purpose of the Regulation is to produce a common regulatory system which creates frameworks for secure, efficient use of electronic communication with and within public administration. The Regulation shall promote predictability and flexibility, as well as facilitating the co-ordination of practical technical systems, including e-signatures.

The E-administration Regulation contains provisions governing routines and procedures connected with archive construction.

The Security Act
Act No. 10 of 20 March 1998 relating to Protective Security Services (in Norwegian)

http://www.lovdata.no/all/hl-19980320-010.html

The Security Act contains a separate chapter relating to information security.

The purpose of the Act is to use preventive measures to safeguard state security and vital national security interests against espionage, sabotage and terrorist acts, and it applies to public administration as a whole. The Act shall moreover ensure the legal protection of individuals, strengthening confidence in and simplifying the control of the service. The measures shall be implemented in state, municipal and those private enterprises to which the Act applies.

Regulations have been prepared relating to information security, personnel security, industrial security and security management. The regulations relating to information security is particularly relevant with regard to archive-related processing of documents in accordance with the Security Act.

Information which shall be protected in accordance with the **Security Act** has the following security classifications:

- **RESTRICTED** is used for information whose disclosure to unauthorised parties may to some degree entail detrimental effects on the security of Norway or its allies, on relations with foreign powers or on other vital national security interests.
- **CONFIDENTIAL** is used for information whose disclosure to unauthorised parties can damage the security of Norway or its allies, relations with foreign powers or other vital national security interests.
- **SECRET** is used for information whose disclosure to unauthorised parties can seriously damage the security of Norway or its allies, relations with foreign powers or other vital national security interests.
- **TOP SECRET** is used for information whose disclosure to unauthorised parties can cause critical damage to the security of Norway or its allies, to relations with foreign powers or to other vital national security interests.

The Information Security Regulation
Regulation No. 744 of 1 July 2001 relating to information security
http://www.lovdata.no/for/sf/fo/xo-20010701-0744.html

The Regulation has the same purpose and scope of application as the Security Act.

The Protection Decree
Regulation No. 3352 of 17 March 1972: Instructions for handling documents which call for protection for other reasons than those specified in the Security Act and associated regulations (in Norwegian)
http://www.lovdata.no/for/sf/in/xm-19720317-3352.html

The instructions for handling documents which call for protection for reasons other than those specified in the Security Act and associated regulations apply to documents irrespective of the medium in which they are accessible.

Protection of a document in accordance with the Protection Decree shall only take place when the document can be exempt from public disclosure pursuant to the Freedom of Information Act and detrimental effects may arise.

Information which shall be protected in accordance with the **Protection Decree** has the following levels of classification:

- **CONFIDENTIAL** is used for documents the disclosure of whose contents to unauthorised parties could harm public interests, a company, an institution or an individual
- **STRICTLY CONFIDENTIAL** is used for documents the disclosure of whose contents to unauthorised parties could lead to substantial damage to public interests, a company, an institution or an individual.

Parliamentary White Paper No. 8 (2012 – 2013). Export of military equipment from Norway in 2011, export control and international non-proliferation co-operation (in Norwegian)

http://www.regjeringen.no/nb/dep/ud/dok/regpubl/stmeld/2012-2013/meld-st-8-2012--2013.html?id=707794

The Norwegian Government's Parliamentary White Paper on the scope of export of military equipment. The document also explains Norwegian export control policy, the regulatory system and international efforts with regard to export control and non-proliferation. Section 3.3 deals with control with regard to the transfer of knowledge to foreign students at Norwegian educational establishments.

References

[CBPD122] Recommended ICT Security Architecture in the Higher Education Sector
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs122.pdf

Glossary

BIA	Business Impact Assessment
Difi	Agency for Public Management and eGovernment
ECON	Finance and economy
ENT	Enterprise critical value
FAD	The Norwegian Ministry of Government Administration, Reform and Church Affairs
HE	Higher education
HIST	Historical value
HSE	Health Security Environment
LEG	Legal value
LT	Lifetime related
Noark	Norwegian archive standard
PERM	Permanent
PERS	Personal
RAV	Risk and Vulnerability Assessment
REV	Review
R&D	Research and Development

Complete BPDs available at www.terena.org/campus-bp/

campus-bp-announcements@terena.org