IT Rules and Regulations for UMB

May 12, 2005

Based on
«IKT-reglement for institusjoner i utdanningssektoren»
UNINETT FAS/UNINETT ABC
Versjon 1.0, 1. desember 2004

Table of Contents

General rules for use of IT 3

Detailed regulations

1. Ownership and treatment of data 5
2. Delivery of logs or similar information 7
3. Use of resources 8
4. The user’s duty to identify himself 10
5. Sanctions against users 11
8. Corrective actions 12
7. User registration 14
8. Handling of cases 15

Appendix

Defined user categories at UMB 17

General rules for use of IT

Applicability:

These regulations apply for the use of UMB's IT resources. They are also valid for use of third party IT resources by means of a connection to UMB's resources

Use of IT resources:

Use of UMB's IT resources is only for the purpose of satisfying UMB's purposes and goals. It is forbidden to use UMB's IT resources for purposes that are in conflict with UMB's goals and objectives or ethical or moral standards which are in force at UMB. Use of UMB's IT resources in conflict with Norwegian law can result in sanctions directly from UMB.

It is not permitted to use UMB's IT resources before permission is obtained. The attainment of a user status at UMB implies that permission is given to proper use of resources.

It is not permitted to use UMB's IT resources in a way which demands greater resources than necessary considering the amount of available resources. Use which does not have its basis in UMB's goal and objectives shall only occupy negligible resources.

IT resources shall not be used in a way which can reduce their integrity or effectiveness. This applies also when private equipment is employed.

Users are required to follow IT employees' orders and instructions concerning the use of IT resources. When asked to do so, a user shall identify himself in a correct fashion. A user's password or other key shall be kept secret from other parties and only be employed by the proper user.

Users shall behave in an acceptable fashion when using the network – netiquette.

Rights of the user

UMB shall provide clear standards and regulations for what is proper use of UMB's IT resources.

UMB shall provide up-to-date information relevant to IT resources and their proper use.

All users are entitled to privacy and that their data's integrity shall not be violated by UMB. UMB shall contribute to the maintenance of their privacy and that their data's integrity shall not be violated by other parties.

UMB shall not provide information on individual users or user's data except where required by regulations or legal practice.

Sanctions and actions by the IT group to enforce these regulations

Violation of the IT Rules and Regulations can lead to sanctions from UMB. Punishment or sanctions due to such violations shall be similar to sanctions due to other misbehavior at UMB. The proper punishment shall be determined by the responsible unit.

IT operative personnel are responsible for the security of the system functions and system integrity. UMB's IT operative personnel are permitted to take all necessary actions to maintain system functionality. When such actions are required, effected users shall be notified as soon as practicable.

Limit of responsibility:

UMB is not responsible for any loss of data or services or other losses as a result of loss of IT services. UMB shall not remove any user rights or hold the user responsible for actions or lack of actions when the cause is loss of IT services.

Detailed regulations

1. Ownership and treatment of data
2. Delivery of logs or similar information
3. Use of resources
4. The user’s duty to identify himself
5. Sanctions against users
8. Corrective actions
7. User registration
8. Handling of cases

Regulation	Date	Authority	Reference
Ownership and treatment of data	12.05.2005	University Board	UB-case 83/2005

This regulation does not apply to logs or related data which are UMB's property.

Starting point:

UMB considers a file to be owned by the registered owner. Whether this ownership is correct, shall not influence the real ownership in any way.

Ownership of data

UMB considers the registered owner of a file to be that data's owner regardless of where the data is situated. UMB will only allow access to the file by the registered owner except when required to provide access to another part as determined by a Norwegian court of law.

Conflict concerning ownership of data between two parties

If two parties both claim to own a data file, UMB will release the data only to the registered owner. However, if one of the parties threatens court action to establish the rightful ownership of the data, UMB shall be permitted to delay the release of the data for a short period.

If the ownership is not clear, will no one get the data?

If it is not possible to establish the rightful ownership of the data, and more than one party claims ownership, the data will not be released until a Norwegian court has decided the legal ownership.

Delivery of the data when user privileges end

User privileges end due to changed relationship UMB – user

When the user's relationship to UMB ends, e.g. when the study period ends or at the end of employment, the user shall, when deemed necessary, take copies for his own use and then himself remove his data from UMB's IT resources. The user shall have access to his data for a period of three months after his user role ends. During this period the user must receive appropriate warnings that his account will be made void and his data will be removed. After this UMB shall wait an additional three months before the user's account and data are deleted.

The fact that the user's data shall be accessible does not mean that other services will be available.

End of user relationship due to death of the user

When a user dies, the lawful inheritors (estate) take over the user's rights to any physical or other objects. The rights to the contents of any user data pass to the estate.

It must be established that the person or persons who request access to the data are indeed the rightful inheritors. This shall be done by presentation of documents with legal force that legitimate the inheritance claims.

Personal files shall be stored on the user's home area for data. After the user's death any material stored on UMB's personal computers/work stations will be deleted without any pre-inspection.

Procedure for delivery of data

Written declaration

Release of the data requires a signed written declaration where the recipient of the data declares the

following:

- The data has been received
- The delivery does not change in any way the legal ownership
- Any data owned by others shall be delivered to the proper recipient

Archiving

A short transcript (e.g. a log) for the delivery with copies of documents legitimating the proper recipient (legal inheritance documents), the declaration, and other related documents shall be stored in the archive.

Delivery

The delivery is done on an appropriate data medium which can be exchanged for the declaration.

Regulation	Date	Authority	Reference
Delivery of logs or similar information	12.05.2005	University Board	UB-case 83/2005

Release of information

It is expected that UMB will occasionally receive complaints or requests for the delivery of logs or information on, or the identity of, a user. Normally shall no such information be released. Much of this information is protected by rules of confidentiality. Rules of confidentiality and the Personal Data Act require the utmost caution concerning the release of information about individuals or their use of IT resources.

Concerning release of information to the police or other trial authorities

As warranted in the Law on Electronic Communication §2-9 police or other trial authorities can demand the identification of a user of an IP number. Other data, e.g. logs of traffic data or contents of communications, require a court order.

Delivery of information to other parties

Release of information, logs or similar data to other parties than police or trial authorities requires a court decision.

Release of information to the user himself

A user can request delivery of information, logs or similar data concerning his own activity by contacting the IT department. This right is authorized in the Personal Data Act.

Shared IT services

Concerning shared IT services including the use of other institutions' IT resources, misuse will be handled by the user's own institution if UMB resources have been misused or UMB itself can process the case in the courts and thereby get access to the user's identity as described in the regulations above.

Regulation	Date	Authority	Reference
Use of resources	12.05.2005	University Board	UB-case 83/2005

Starting point.

Use of UMB's IT resources shall be used principally to advance UMB's goals and objectives.

It is not permitted to use UMB's IT resources in a way that occupies greater resources than necessary considering the available resources. Use which is not based on UMB's goals and objectives shall only occupy negligible resources.

Use according to UMB's goals and objectives.

UMB's main objectives are the provision and advancement of education, research, and the communication of information.

Use of IT resources directly related to UMB's goals and objectives is the basis for the resources which are available and such use is therefore permitted provided the extent of the usage does not prevent others from other responsible usage.

Use not directly related to UMB's goals and objectives is only permitted to that degree that the resources occupied can be considered negligible. Use which does not have defensible interest can by forbidden by the IT department.

Private use

IT services at UMB are principally to be used to advance UMB's goals and objectives. However, it is allowed to employ IT resources for private purposes provided that this use

- does not occupy IT resources in such a way that it prevents other usage.
- does not invalidate licenses or other agreements
- does not weaken security or system stability
- is not forbidden by the IT department

Commercial use

Use of UMB's IT resources commercially (all forms of buying, selling, renting, or marketing for personal gain) is forbidden unless written permission to such activity has been obtained in advance.

No defensible interest

Actions which employ IT resources, but are not based on defensible interest such as UMB's goals and objectives or other commonly accepted interests, can be forbidden by the IT department. In cases where there is reason to critisize the user for his actions, sanctions can be implemented. The following shall be taken into consideration:

An action does not have defensible interest if it is not close to UMB's goals and objectives nor is it in line with generally accepted rights or goals such as:

- democracy
- basic human rights
- society or community use and interest

- technical or other scientific progress

Actions could be in conflict with these regulations concerning use of UMB's IT resources.

The IT department can employ sanctions against a user which has performed an action which:

- Most users would have understood that the action was not an acceptable use of IT resources

and

- The action was not restricted to the user's private domain.

Enforcement of resource use regulations.

Each department and individual user has independently a responsibility to assure that his own use is within the limits permitted by these regulations. The IT department can and shall provide general directives on what is acceptable use.

In special cases where the IT department becomes aware of questionable use, it will take into account the nearness to UMB's goals and objectives, other defensible interests, and the volume of resources occupied. If after these considerations the use is considered unacceptable, the IT department will take steps to stop the activity. If there is reason to criticize the user for his use of resources, sanctions against the user can be instituted by the IT department.

Regulation	Date	Authority	Reference
The user's duty to identify himself	12.05.2005	University Board	UB-case 83/2005

Correct identification

All users shall, whenever required, identify themselves for UMB in a correct manner. It is forbidden to give a false identification or attempt to do so.

Correct user name

For all services at UMB only one's own user name shall be used.

Correct sender address

It is forbidden to attempt to modify or hide any field or information in any communication in order to hide the origin or to give a false impression of the origin.

Correct machine name/IP address

It is forbidden to attempt to change a parameter, access services by circuitous routing or by any other means to hide which machine one is using or give a false impression of this for UMB or other UMB users.

Secrecy of keys

It is very important that a key be kept secret. This exists often in the form of a password or a pin-code. It is forbidden to share this with others. If it becomes clear that a key has been divulged, the user account will be blocked for further use and the user made responsible.

Right to anonymity

It is not UMB's responsibility to determine whether a user identifies himself for a third party when using open services outside of UMB. However, infractions of Norwegian or international law perpetrated by means of or with the aid of UMB's IT resources will be subject to the IT Rules and Regulations.

Regulation	Date	Authority	Source
Sanctions against users	12.05.2005	University Board	UB-case 83/2005

Sanctions

A sanction is a reaction instituted to punish a user for criticizable behavior on the user's part. Actions instituted to achieve other results, e.g. stability and security for IT resources, is not a sanction.

Sanctions related to user behavior with regards to IT resources shal be handled by the IT organization. Sanctions related to other behavior shall be handled by the user's responsible department.

Extent of sanctions and competence to institute them

The University Board

The blocking of a user account is an expulsion in accordance with University Law §11.

The University Board is given authority to expel a user. The process to do this is specified in the laws, which shall be followed in such cases.

The right to an operative user account which gives access to administrative services, education, and related data delivery, examinations, etc. cannot, as a sanction, be denied a user without this being considered an expulsion. The same applies to the ability to receive communications from UMB or any of its organs.

Responsible unit

The responsible unit shall not institute sanctions by changing privileges for use of IT resources.

IT organization

The IT department can institute sanctions by retracting certain limited privileges for a limited amount of time.

Sanctions shall be a result of a misuse and be related to the misused resource.

The first echelon of the IT organization shall not institute sanctions against users above verbal correctives or reporting of the users to the second echelon.

In the case of serious misuse the IT department shall escalate a case in the chain of authority via the responsible unit to the University Board, which decides whether expulsion shall take place.

Regulation	Date	Authority	Reference
Corrective action	12.05.2005	University Board	UB-case 83/2005

Corrective action

A corrective action is an action taken for a different purpose than to punish a user.

The IT department can take corrective actions when necessary to maintain security, integrity, confidentiality, and accessibility of IT systems, to prevent loss of life, health, or property, to limit UMB's economic responsibility, to maintain UMB's reputation, or to prevent illegal actions.

Exceptional access

Exceptional access is the case where a person, by means of some manual process, gains access to data belonging to another user. Automatic processes which take actions directed towards large groups of users do not make exceptional accesses. This applies to e.g. virus scanning or processes that generate reports which do not identify individuals.

Files, user areas, and logs

The user's private area extends only to knowledge about the existence of and contents of files. Which processes a machine is running is information which shall be accessible at any time by operative personnel.

Logs which contain information about processes, users logged in, deviations or other occurrences or events are UMB's property and shall be accessible by operative personnel.

There is a definite separation between the user's files and areas, and the logging of various things by an institution. It is not exceptional access as such to look through these, but it must be such that UMB only logs that which is reasonable and users shall be informed about these things.

Exceptional access to data, files or areas belonging to a private user

As a starting point only the user himself has access to his own data, files or private data areas.

Consent

It is normal that a user's consent shall be requested if corrective actions with exceptional access are necessary.

In some cases it may be necessary to make an exceptional access without consent.

Permission granted by superior

In a situation where it is necessary to act quickly or other aspects make it impossible or very difficult or counterproductive to request consent, exceptional access can be performed with permission from the IT director or his authorized deputy.

Extremely time-critical situations

In extremely time-critical situations or when other causes make it impossible or very difficult or counterproductive to obtain permission from the IT director or his authorized deputy, exceptional access can be made by the IT personnel.

Information provided after exceptional access

Whenever exceptional access into a user's private data area has been performed without obtaining his consent in advance, the user shall be warned at once.

The warning shall describe the action taken, the authorization for this and the special conditions that made this necessary.

Registration of exceptional access

The exceptional access shall be registered in the case handling journal.

Blocking/denial of resources

When deemed necessary corrective action can be performed by blocking, denial or in some other way changing a resource.

Information to users

When a resource has been blocked or denied, the user shall be informed. This shall be done as soon as possible. When resources which effect many users are blocked or denied, the content of the warnings can be identical. If practical the information should be provided individually to the affected users. The message shall be given via a communications medium which is not itself blocked.

Regulation	Date	Authority	Reference
User registration	12.05.2005	University Board	UB-case 83/2005

Necessary requirements to become a user

To become a user at UMB it is necessary to have a formal relationship to UMB. A formal relationship is employment, acceptance as student, or a written agreement allowing presence at UMB.

To become a user a minimum set of one's personal data shall be available in one of the administrative systems at UMB. This system can be the student information system or the personnel system. The information which must be registered is:

- name
- Norwegian Identification Number
- relationship to UMB
- duration of the relationship
- location at UMB

Certain types of employees can have relationships which do not strictly require use of IT services. In such a case objective criteria shall be used and selection shall based on formal roles at UMB. This shall be made clear in the registered information in the student information system or the personnel system.

Registration of users

At the time of registration of new individuals in either the student information system or the personnel system a user entity shall automatically be made for the person. This does not apply if:

- *it is clear from the registration that this person shall not have user privileges*
- *a user entity already exists for a person with this identification*

If a user entity already exists and this shall be used, it must be checked that the required personal information listed above has been updated.

After the user entity has been created, user name and password (or other authentication information, e.g. pin-code) shall be sent to the user at his place of work or student address. At the same time the user shall receive information concerning IT resources and rules for their use.

The IT department shall as a rule not make a user entity for a person not found in the student information system or personnel system. Exceptions can be made where technical requirements make this necessary. Also in the case of manual registration the obligatory personal information listed above shall be registered. Manually registered users shall not be valid for more than one year.

It is permitted to require that a user choose a new password/pin-code the first time he uses or activates his user account.

Duration of user relationship

The duration of a user's account at UMB shall be as long as his relationship to UMB. In addition the user can have three months time to dispose of his files before the account is closed.

Cessation of user relationship

When the user's relationship ends after registration in either the student information system or the personnel system, the user shall be warned that his account will be closed in three months and that the user during this period must take security (archival) copies of all files he wants to keep[1].

After three months the user account is blocked. After an additional six months the user account is closed. Archived security copies are deleted after five years.

[1] See section "Ownership of data"

Regulation	Date	Authority	Reference
Handling of cases	12.05.2005	University Board	UB-case 83/2005

General rules for case treatment

IT employees are governed by the general case handling rules for public employees concerning exercise of authority for employees in steering and management functions.

Professional secrecy

IT employees are subject to the code of professional secrecy in accordance with the Public Administration Act § 13. The code of professional secrecy applies to all applicable case information which the employee receives in the capacity of his position. The code of professional secrecy applies also towards other employees in the IT organization except superiors.

Archival storage responsibility

Documents belonging to an individual case in accordance with the Public Administration Act §2b require archiving and the archiving shall be done in a public journal. When there is some question as to whether a case requires archiving, archive personnel shall be consulted.

Right to information

All are entitled to be informed of the contents of public journals in accordance with the Law of Public Information § 2.

All parties in a case have the right to view the case documents. This right does not apply to documents and communication for internal case preparation.

Obligation to reply

UMB is obliged to reply to all inquiries received in its capacity as a public institution. This does not apply to indiscriminate communications sent out as part of advertising or marketing campaigns e.g. SPAM.

All inquiries shall be answered within a reasonable amount of time.

UMB is obliged to provide general counseling to users related to these inquiries. Such counseling can be reference to available information. In cases involving exercise of administrative functions the inquirer shall be informed of his right to make an official complaint concerning a decision in an individual case.

Repeated inquiries are not permitted in cases which have been concluded and where the right to further complaints or appeals does not exist. Further expressions of opinion in such cases are not permitted. It is not required to reply to such communications and they can be answered with a standardized rejection.

Electronic communication

It shall be stated clearly, for example on UMB's internet homepage, where inquiries can be addressed for electronic communication. The communications channels which are listed there shall be read by humans and not be subject to automatic deletion of communications.

Appendix to the IT Rules and Regulations for UMB

April 25, 2005

Defined user categories at UMB

Starting point:

This appendix to the IT Rules and Regulations defines which user categories presently exist at UMB in relation to the IT Rules and Regulations Detailed Regulation no. 7: User Registration.

This appendix can be changed when necessary.

Defined user categories:

Employee

Description:	User employed by UMB
Authorizing unit:	Personnel administration, Salary and personnel system
Level of rights:	Basis - Fagnett (vLan10). Group membership can give further rights
Durtion:	Unlimited. Ends when employment ends. (ref. Paga)
Closure procedure:	Accounts closed at termination of employment. Personal data (ref. Detailed Regulation 2) shall be the responsibility of the user until termination of employment. After closing of accounts, if mutually agreed, available for three months. After this the data shall be archived for up to one year after termination date.
Comment:	Shall not be used for short-term contracts of up to one month. Stipend recipients employed at UMB are considered employees.

Student

Description:	User having a student relationship to UMB, including stipend recipients.
Authorizing unit:	Study department, FS (“Felles Studentsystem”)
Level of rights:	Student network (vLan30).
Duration:	Unlimited. Ends when student relationship ends (ref. FS).
Closure procedure:	Accounts closed at termination of student relationship. Personal data (ref. Detailed Regulation 2) shall be the responsibility of the user until termination. After closing of accounts, if mutually agreed, available for three months. After this the data shall be archived for up to one year after termination date.
Comment:	Stipend recipients who do not have an employment contract with UMB who need additional rights must also be defined as “associate” category.

Associate

Description:	User with a negotiated connection to an UMB unit, where there is need for a place of work at UMB.
Authorizing unit:	The unit which was a party in the agreement.
Level of rights:	As agreed between the parties.
Duration:	Limited. Duration up to two years. In case of renewal, a new time limitation shall be made.
Closure procedure:	Accounts closed at termination of relationship. Personal data (ref. Detailed Regulation 2) shall be the responsibility of the user until termination. After

	closing of accounts, if mutually agreed, available for three months. After this the data shall be archived for up to one year after termination date.
Comment:	The category ”associate” entails more responsibilities than ”guest”. The authorizing unit is therefore required to have a written agreement which describes the user’s function and needs while at UMB.

Guest

Description:	User with a short stay at UMB.
Authorizing unit:	Unit which has invited or in some other way has an agreement with the user.
Level of rights:	Only ”the guest network” (vLan 95).
Duration:	Limited.
Closure procedure:	No account is established and there is therefore no data to be removed.
Comment:	

Course participant

Description:	Participant of a ”further education” course (no FS connection).
Authorizing unit:	SEVU / unit responsible for the course.
Level of rights:	Logon in the data room.
Duration:	Limited to the duration of the course.
Closure procedure:	Accounts closed at termination of the course. No personal data will be archived.
Comment:	

Retired

Description:	Retired employee of UMB who has an agreement concerning a place of work at UMB.
Authorizing unit:	The agreeing unit.
Level of rights:	As agreed.
Duration:	Limited, maximum two years. At each renewal a new limit shall be set.
Closure procedure:	Accounts closed at termination. Personal data (ref. Detailed Regulation 2) shall be the responsibility of the user until termination. After closing of accounts, if mutually agreed, available for three months. After this the data shall be archived for up to one year after termination date.
Comment:	The category belongs under ”associate”, but is so frequently used that it is appropriate to have its own category and where the contract requirements are more limited.

IT-adm

Description:	User at the IT department’s administration.
Authorizing unit:	Concerned unit.
Level of rights:	Fagnett (vLan10) + administrative rights.
Duration:	Limited, maximum two years. At each renewal or change a new limit shall be set..
Closure procedure:	Accounts closed at termination. Personal data (ref. Detailed Regulation 2) shall be the responsibility of the user until termination. After closing of

accounts, if mutually agreed, available for three months. After this the data shall be archived for up to one year after termination date.

Comment: The category belongs under ”associate”, but is so frequently used that it is appropriate to have its own category and where the contract requirements are more limited.

Functional user

Description: User account related to a job function rather than person. The account is independent of personal accounts and can be used by several persons in a group. The account must nevertheless have one responsible owner.

Authorizing unit: Concerned unit.

Level of rights: Dependent on the job function.

Duration: Unlimited, but is tied to the responsible owner.

Closure procedure: The account is deactivated when the responsible owner’s relationship terminates. No personal data is connected to the user account.

Comment: