LEGAL BULLETIN

OF NICOLAUS COPERNICUS UNIVERSITY IN TORUŃ

2017

Resolution No. 196

Of the Rector of Nicolaus Copernicus University in Toruń

of 19 December 2017

On the basis of article 66(2) of the Act of 27 July 2005 on Higher Education Law
(Journal of Laws of 2016, item 1842 with further changes).

it is resolved as follows**:**

Chapter 1
General definitions

§ 1

1. At Nicolaus Copernicus University in Toruń, herein referred to as 'NCU' a computer network is operating.
2. NCU Computer Network, herein referred to as 'NCU CN', encompasses all NCU objects, especially localizations in Toruń, Piwnice and Bydgoszcz as well as network services made available by NCU on own or foreign resources.
3. NCU CN basic role is to support didactic, scientific and NCU management processes.
4. NCU is not responsible for damages caused by NCU CN malfunction.
5. NCU CN may be used in a manner not breaching any applicable legal regulations.
6. Any content or images of commercial, advertising, political etc. nature cannot be distributed through NCU CN without the Rector's or the Chancellor's previous consent

§ 2

1. NCU CN safety policy, herein referred to as 'Policy' is implementing uniform rules of actions of network and services users and administrators in order to ensure proper data protection.
2. The Policy encompasses the essential document is issued as a Resolution of NCU Rector as well as 3 appendices determining detailed procedures of action in these areas of NCU CN:

1) Managing account – appendix 1;
2) Managing domains – appendix 2;
3) External services disseminated through NCU CN account– appendix 3.

3. NCU IT Centre, herein referred to as 'UCI' is responsible for maintaining the Policy, especially for submitting proposals for actualisation resulting from changes of law and technology.
4. Internal documents, specifying detailed rules of action of subsystems creating NCU CN, approved by the UCI Director accompany the Policy.
5. If the word **should,** or its variations, are used in the text, it has to be interpreted as an injunction which may have some exceptions in particularly justified cases. Such exceptions has to be documented.

§ 3

1. Dedicated networks for guest access such as e.g. a part of eduroam network or part of conference service network dedicated for external users, are treated as external resources towards NCU CN and movement from this network directed to other parts of NCU is filtered on the same grounds as the movement outside NCU.
2. Dedicated networks for guest access have to have own regulations available at least in both languages – Polish and English.

§ 4

1. NCU's main domain is umk.pl which means that at general academic websites as well as NCU websites of Faculties and Departments other academic websites are addressed only through this domain.
2. The right to request for registration of websites in umk.pl domain have only: Rector, Chancellor, Deans, Heads of institution-wide and interdepartmental units.
3. Each name registered in umk.pl domain has to have an appointed supervisor.
4. Names in umk.pl domain are registered by the administrator of NCU CN upon written request of an authorized person.
5. Period of domains validity and their closure procedure is determined in appendix 2.

Chapter 2
NCU CN Users

§ 5

1. NCU CN user is every person who uses a device linked to NCU CN or network service of NCU CN.
2. In order to access the protected sources of NCU CN is vital to own a user's account of NCU CN herein referred to as 'NCU CN account'.
3. NCU CN account additionally gives authorizations of using given external services determined in External services use regulations, an appendix 3 to this Resolution..
4. In some cases, the access to specific services requires special accounts connected to services. This account is called an account in service.

§ 6

1. NCU CN account is a registered authorization to NCU CN use.
2. NCU CN accounts may be owned by:
   1) NCU employees employed by employment contract or a civil law contract;
   2) NCU retirees and pensioners;
   3) Other persons who need an account in relation to classes conducted at NCU or participation in NCU courses, internships etc.
   4) NCU students (and doctoral students);
   5) NCU guests during their stay at the University;
   6) NCU owners of Graduates Card;
   7) Other persons – especially in justified cases, after UCI Director's approval
3. At general academic servers one person may own only one NCU CN account.
4. Employees, retirees, pensioners and NCU students have the right to keep own WWW website held accordingly to §(6).

§ 7

1. Procedures concerning NCU CN account service are determined in Appendix 1.
2. NCU CN accounts of Graduate Card owners are held according to the rules determined by the regulations of Graduate Program.
3. NCU CN account used with violation of §1(5) is blocked by the administrator of NCU CN or administrator of a specific local network. An appropriate supervisor of the user is informed about the fact of blocking NCU CN account. After explaining the situation, the supervisor makes a decision about unblocking the account.
4. Additional rules for maintaining NCU accounts of users in local networks of NCU CN may be determined in these networks regulations.

§ 8

1. NCU CN accounts of persons who have lost their authorization for the account expire and are deleted after the account validity period foreseen for this type of account.
2. The administrator informs the user, who has lost the status authorizing to ownership of NCU CN account, about the date of account deactivation via email.
3. Neither identifier, nor paired with it electronic mail aliases of a deleted NCU CN account will be assigned to another person.
4. The deadlines and procedurę of NCU CN account deletion are described in appendix 1.

§ 9

1. Function account is an authorization to implement tasks or a provision of information services for:
   1) NCU organizational units;
   2) student and self-governing organizations functioning in NCU;
   3) student scientific groups;
   4)other institutions and organizations, made available upon separate regulations or arrangements.
2. NCU organizational units function accounts are maintained on commission of their Head.
3. Function accounts of student and self-governmental organizations as well as student scientific groups are maintained upon their request accepted by the Rector or a Dean.

4. Each function account has to have a supervisor appointed by an appropriate person for creating such accounts.
5. Function accounts may be used only accordingly to the purpose for which they have been created.

§ 10

1. Account in service is an authorization to access to the service which does not use NCU CN account system.
2. Services may define own regulations concerning requirements in relations to accounts in service, in particular concerning the way of logging into the service, requirements concerning quality and frequency of password change etc.
3. Service may define own rules concerning the time of account validity and the procedurę of their deletion.

§ 11

1. Email addresses ID@umk.pl or ID@cm.umk.pl where ID is an identifier meeting the requirements of email may be assigned only to NCU CN accounts of employees, retirees and pensioners of NCU and people determined in §6(2) point 3 and function accounts.
2. NCU employee using NCU CN account on a general academic server receives by default an email address ID@umk.pl or ID@cm.umk.pl where ID is the account identifier; during creating of the account, the employee is informed about the possibility of defining additional email addresses.
3. Doctoral students using NCU CN account at NCU general server use email address ID@doktorant.umk.pl, where ID is doctoral student account identifier.
4. Other students using NCU CN account at the general academic student server use email addresses ID@stud.umk.pl where ID is an identifier of student account.
5. NCU guests during their stay at the University use NCU CN account at NCU general academic server (accordingly to its Policy) use email address ID@v.umk.pl where ID is an account identifier.
6. Owners of NCU Graduate Card use email address specified by the Graduate Program regulations.
7. Users of NCU CN accounts at local servers use email address determined on the basis of regulation concerning those servers.

§ 12

1. NCU employees are obliged to use work email address for work correspondence.
2. It is not advised to configure automatic forwarding of mail received at the NCU email address to servers outside NCU. UCI is not responsible for problems connected with receiving mail if the account has a forward to a server outside NCU configured.

§ 13

1. In order to protect the network, the user of NCU CN is obliged to care for safety of own accounts, especially to protect own passwords and other data serving the authorization process.

2. The user cannot request a change of a password or opening blocked access via phone call if there is no possibility of identification of the caller.
3. NCU CN must not:
   1) Allow others to use his/her account and authorizations resulting from it;
   2) Make attempts to use an unknown account and starting an application deciphering passwords
   3) Take actions in order to intercept or eavesdrop information distributed by the network;
   4) Change of assigned IP address of devices (except for situations agreed upon with an administrator of a particular network);
   5) Run applications which may disturb or destabilize the work of a system or computer network as well as invade privacy of system resources;
   6) Send mass email towards random recipients (spam).
4. In case of not respecting the rules above by the user, the administrator may limit or block the access to the network or a service temporarily.

§ 14

1. The content of user's account, especially content of post box, is protected with professional confidentiality.
2. In justified cases, under Rector's or Chancellor decision, the content of the account may be enclosed to third parties.

Chapter 3
NCU CN description

§ 15

NCU CN components in Piwnice and Toruń:
1) A network of servers of NCU central services administered directly by UCI serving various types of services and requiring different types of;
2) Internal UCI network encompassing UCI employees workstations divided into areas of access;
3) NCU administration network, administered by the Computerisation Office of UCI University Administration (PKAU UCI), mostly using separate rooms and cable infrastructure or dedicated transmission channels within TORMAN network;
4) Local networks of NCU organizational units in general having a territorial and address identity (separate IP routing) which may be administered by their home units or their administration may be entrusted to UCI. Organizational units networks are attached through edge devices of TORMAN network ;
5) NCU wireless network under UCI management;
6) the network of student homes and assistant hotels.

§ 16

NCU CN components in Bydgoszcz:
1) NCU CN local networks administered straight by CM IT department providing services of all kind and requiring different types of access for users, divided into sub areas both

logically as well as geographically. Local networks may function through devices and infrastructure of BYDMAN network;
2) NCU CM local administration network administered directly by CM IT department connected to central cable infrastructure;
3) networks of organizational units in general being a part of NCU CN local networks having, in specific cases, address identity, may be administered by home units or administration may be entrusted to CM IT department;
4) NCU wireless network under CM IT department;
5) the network of student homes and assistant hotels.

§17

Managing network in NCU localizations other than those referred to in §15 and §16 depends on the status of localization and has to be regulated by proper authorities for the particular localization.

§ 18

Dependance of NCU CN on external factors:
1) NCU CN uses links of the TORMAN and BYDMAN network as well as other telecommunication links both through using dedicated optical fibres as well as digital channels;
2) Present policy does not regulate TORMAN network matters and treats it as an external object; however, it presents expectations towards access of TORMAN network and other operators resources;
3) In justified cases NCU CN may use commercial operators services.

§ 19

1. UCI performs the function of an administrator of NCU CN on behalf of which these entities operate:
   1) outside Collegium Medicum - the head of the UCI Academic Network Office or other person authorized by the head of the UCI;
   2) at the Collegium Medicum - the head of the CM IT department or other authorized person.
2. The head of the organizational unit having a local network appoints an administrator of the network and informs about his/her decision the head of the UCI.
3. The administrator of local network is responsible for its exploitation cooperating with NCU CN administrator.
4. The administrator of local network keeps NCU CN accounts on computers in his/her network and is responsible for guaranteeing that the rules of operating the accounts were in line with § 6.
5. The administrator of local network is obliged to guarantee that the plug sockets protection was realised in line with § 41.
6. The administrator of local network cooperates with NCU CN administrator in order to maintain continuity, cohesion and safety for NCU CN.
7. Administrators appointed by the Chancellor in consultation with the head of the UCI and cooperating with the head of the Student House Department and Assistant Hotels manage the student houses and assistant hotels network.

Chapter 4
Physical protections and resistance to malfunctions

§ 20

1. NCU CN should be realised in an malfunction-free manner ensuring automatic switch to backup systems. The realization of this rule must take into account the balance of costs and risk analysis.
2. Single malfunction points as well as systems the switch of which does not occur automatically must be inventoried and the manner of reaction to their malfunction must be prepared and appropriately documented.
3. NCU CN main points, especially localizations in which the servers were put, must be connected with more than one optic fibre track so as to ensure continuity of system's work in case of one optic fibre track's malfunction.

§ 21

1. Central services are realised with ensuring rules of lack of malfunctions taking into account data distribution both logically as well as geographically.
2. Realization of services includes their smooth transfer to other server in an automatic mode or one requiring administrator's intervention. The choice of protection method, determining maximum permissible malfunction period depends on service criticality and is described in internal document [servers refundation].

§ 22

1. Servers, data storage matrixes, network server switches are placed in a few independent localizations herein referred to as server rooms, giving possibility for resource migration.
2. Server rooms are closed, air conditioned and placed in buildings with supervision of porters or with electronic supervision. The access to rooms is limited to a group of authorized administrators. It is advised for the server rooms to have electronic locks connected to entrance recorder.
3. Persons who clean the server rooms have to have an authorization as well as proper training, all of it has to be documented.
4. Renovations and repairs conducted in server rooms are previously consulted with administrators and are under their supervision.
5. Server rooms should be monitored with a help of cameras registering at least the moment of entering the room.
6. Servers, matrixes and switches are attached to the grid protected with devices such as UPS and, if possible, with power generators.
7. Virtualization servers, matrixes and switches realizing a cluster of servers are located so as to each element has a backup component placed in a server room powered from emergency power generator.
8. Key devices are equipped with multiplied power supply connected to separate circuits.
9. Air conditioning of the server room has to provide maintenance of temperature enabling work for devices for at least 4 hour period also during lack of external power.

10. UPS devices and emergency generators are under the procedure of efficiency tests described in internal document [server rooms].
11. Internal document [server rooms] contains a list of server rooms along with the description of their protections.

Chapter 5
Protection of data and services

§ 23

The unit responsible for functioning of basic network services and coordinating actions regarding providing access to network services in NCU CN is UCI, and in case of local services, in Collegium Medicum - CM IT department.

§ 24

1. Service servers (physical or virtual) are placed in a separate virtual networks depending on realised functions by them as well as the manner of access for the users. Especially servers to which users can log into, strat their own programs, websites and services are placed in a dedicated network. The list of dedicated subnetworks and service servers division is described by the internal document [servers subnetworks].
2. The access to central services servers network as well as administration servers is protected by the firewall systems. The rules of access to firewall configuration, documentation of implemented changes and firewall refundation are described in internal document [firewall].
3. The access to virtual servers is protected with a system o passwords accordingly to the rules described in chapter 9 of present document.

§ 25

1. The responsibility for realization of proper data kept on servers protection is carried by the designated administrators.
2. The data kept on servers must be protected in a way adjusted to specific needs.
3. Significant data should be protected from their loss, unauthorized modification and accidental deletion.
4. If on the basis of specifics of shared resource or service or the character of data keeping it is valid to apply lower level of protection that the one referred to in the article 3 the users of these resources and services are informed about the level of risk.
5. In case of keeping a few copies of data, they have to be kept at different localizations.
6. Specific rules of keeping backups depend on specific systems and are described in internal document [rules for creating backups].
7. Every system of backups must be equipped with description of action and description of procedure of data recovery. The description of the procedure of data recovery must be easily accessible also in case of wide IT system malfunction.

§ 26

1. In system logs there are information on system operation and on users activity.
2. System logs concerning key elements of system safety are automatically created at the logs central system so that in case of hacking covering the traces is made impossible.
3. System logs are treated as documents under professional secrecy.
4. The time and manner of keeping the logs depends on their type and is described in detail in the internal document [instruction on keeping system logs], whereby it is a subject to general rules:
   1) logs containing information on activity of users are kept no longer than 1 year an are automatically deleted after that;
   2) longer keeping of extracts from system logs created for statistical purposes is permitted, these extracts should not contain information helping to identify the user's activities;
   3) particular IT services may, in justified cases, keep own logs for longer period of time - the information is placed in politics of privacy published by a given service.

§ 27

1. Physical servers, matrixes, network devices, virtual servers and central services are monitored by a special software.
2. In case of service malfunction, the monitoring system attempts to automatically restart the service.
3. Information about critical malfunctions are sent via email and by an additional channel of communication e.g. text message to the entire group of administrators responsible for a particular area of action.
4. Monitoring of availability of services and servers should be realised by at least two servers placed in different localizations and an additional channel of communication, referred to in article 3, should enable sending the message without NCU CN part taking so as to make message system independent from NCU CN components malfunctions.

§ 28

1. Servers of services must be updated through installation of current safety improvements.
2. In case of receiving an information about occuring danger, UCI sends information to an appropriate group of recipients; however, it does not release NCU CN subnetwork administrators from responsibility for safety of networks administered by them.
3. A significant attention is paid to dangers influencing safe communication between users and servers, administrator's tasks is to keep an appropriate level of safety even if that means to limit the access to some devices for users.

§ 29

Administrators have the right to limit the amount of server resources shared and in justified cases, they may limit the access to network services, operations such as starting a program, saving/reading project files or connecting to other systems.

§ 30

1. Services made available by the network launched on NCU CN servers must use a safe software.
2. In case of order of creating a software realizing services available through the network, e.g. creating a WWW service, the authorising officer must guarantee that he/she will reserve funds necessary for ensuring support for the software for the entire period of its exploitation.

§ 31

1. In case of an assumption that unauthorized persons had the access to the server, the administrators take necessary reparation steps.
2. Any cases of breaching access rules are registered.
3. If the unauthorized access concerns user's account, the administrators block the account and, if possible, inform the user.
4. If an unauthorized access concerns the level of server management, the administrator of the server should check logs and conduct an audit of system software and subsequently take actions in order to remove the cause of the incident.

§ 32

1. In all cases where the access to the server is connected with safety elements such as logging data transfer, documents management or processing of personal data, the connection between the server and workstation must be made by an encrypted channel.
2. A server providing access to a safe service enforces using an encrypted channel and encrypting parameters must be compatible with current safety regulations.
3. In case of processing of personal data, it is necessary to ensure protection described in Safety Instructions of a particular system of processing of personal data.

§ 33

1. All administrators of IT systems are obliged to keep a professional secrecy. The obligation of keeping professional secrecy is valid also after termination of employment at NCU.
2. Professional secrecy encompasses in particular:
   1) information concerning network configuration and IT systems of NCU;
   2) passwords and other access data;
   3) any personal data;
   4) the content of home catalogues and users' correspondence;
   5) administration data;
   6) system logs containing information on users activity.
3. Providing access to any data covered by the obligation of professional secrecy is possible only upon written request and has to have Rectors, Chancellor's or other authorized persons approval.

Chapter 6
IT services

§ 34

1. UCI maintains academic name server (DNS) for the needs of NCU CN. Providing access to the name server in local network is conducted in consultation with NCU CN administrator.
2. Managing subdomains of NCU on servers located outside NCU CN may take place only in particularly justified cases and requires Rector's consent.

§ 35

1. UCI maintains academic server of email, is responsible for its correct configuration and constant accessibility.
2. Network services launched under names registered in umk.pl domain operate on NCU CN servers. Registration of the domain cannot serve only for redirecting the service on the server outside NCU or embedding the content downloaded from the external server.
3. NCU CN local networks may have own email servers or use academic server. NCU CN administrator has the right to decide on blocking the access to email service in local network after establishing that this service does not operate correctly.

§ 36

1. Server's task that operate email is providing with consignment with concurrent protection of users from spam and consignments containing unwanted software.
2. Consignments recognized as suspicious but not categorized as spam must be appropriately marked so that the user could define own rules of conduct.
3. Users are obliged to comply to the rule of limited trust in particular no to take actions such as providing own password or changing the password in response to a received message.
4. Taking into account the dangers such as sending spam from NCU CN and consequences connected with these actions, email may be sent only through appropriately safeguarded servers.
5. Email sent from NCU CN must be scanned for spam and unwanted software content, consignments recognized as dangerous must be blocked and the user of the account from which the message was sent must be informed.
6. It is forbidden to use internet forms allowing to send email to any recipients.

§ 37

1. Sending email to all employees or students requires Rector's, Vice-Rector's, Chancellor's or authorized person's consent.
2. Consents for sending such email is one-time or permanently.
3. UCI provides the user with the consent with an address enabling to realise the consignment.

§ 38

1. UCI maintains academic server WWW, is responsible for its correct configuration and constant accessibility.
2. NCU CN local networks may have own WWW servers or use academic server. NCU CN administrator has the right to decide on blocking the access to the WWW service in local network after establishing that this service does not operate correctly.

§ 39

1. The administrator of WWW server determines the technical conditions of WWW websites of users maintenance.
2. WWW websites of users serve for educational and scientific purposes and in case of organizational units and organizations for purposes according with their statute activity.
3. The user is responsible for the content placed on his/her WWW website. In particular § 1(5) is applied.

Chapter 7
Managing network layer

§ 40

1. Particular NCU buildings are wired for the purpose of NCU CN connections.
2. Connections between buildings, depending on the situation, may be realised with the help of route and devices of TORMAN network and external networks of telecommunication operators.
3. Monitoring of TORMAN network encompasses both devices of TORMAN network as well as chosen local network devices.
4. Points of network concentration in buildings should be localized in closed, air conditioned rooms and in case of lack of such possibility, the devices have to be installed in lockers. The access to keys must be limited and registered.
5. Building's networks are operated by manageable switches enabling monitoring as well as access control to particular hubs.
6. Connections between hubs of switches and final network slots must be documented.
7. In case of construction projects realisation which range includes modernization or wiring the building, an essential element of acceptance of the investment is a certificate of final acceptance of structural network wiring stating compliance of wiring with expected norms and receiving full as-built documentation of the structural network.

§ 41

1. Attaching devices to the wired network being a part of NCU CN is under protection.
2. Network ports in areas publicly accessible are configured in a way allowing the identification of a user of the port.
3. A minimum requirement of protection in rooms with limited access is control of addresses assigned by the DHCP server and monitoring of the network for appearance of unknown devices.

§ 42

1. NCU maintains central wireless network connected with global eduroam system.
2. The access to eduroam requires having an active NCU CN account authorizing to use a network or an account in other institutions included in eduroam system.
3. NCU CN accounts of NCU employees and students authorize to eduroam network access around the world.
4. NCU CN accounts of NCU graduates authorize to access eduroam only at the premises of NCU.
5. Devices of persons with eduroam account outside NCU as well as owners of NCU graduate account are placed in virtual subnetwork which is treated as an external network towards NCU. In this network, automatic access to e-magazines of which NCU is a subscriber is unavailable.
6. Eduroam serves access to network at the premises of NCU and cannot be used in order to create permanent network connections through e.g. directional antennas and signal amplifiers.
7. In situation creating a suspicion that the account of a user is abused e.g. many devices use one account or the manner of use indicates permanent connection set, administrators may block the authorization for network use.

§ 43

1. Inside NCU CN, unprotected wireless networks run is forbidden.
2. Access devices of wireless connection may be attached to NCU CN only in consultation with NCU CN administrator or a person authorized by the NCU CN administrator to make such decisions in particular area; connecting devices without consultation will be treated as a serious breach of NCU CN safety.
3. In justified cases, NCU CN administrators may apply methods of strangling unknown wireless devices.
4. Devices using wireless network cannot disrupt work of other network users and users of such devices are obliged to adhere to recommendations of NCU CN administrator.

Chapter 8
Devices of users

§ 44

1. Workstations owned by NCU should be protected with continuously updated software ensuring computer system safety.
2. In case of personal data processing, it is necessary to ensure protection described in Safety Instruction of the particular system of personal data processing.
3. The description of diverse operational system protection is updated continuously and available at UCI websites.
4. The administrator of the software assigned to a particular station is responsible for workstation software safety.

§ 45

In NCU CN private devices may be connected with under following conditions:

1) the user operating private device is responsible for dangers that may occur when his/her device is not properly protected;
2) the user is obliged to a proper protection of own device so as to exclude any unwanted access to services through passwords kept on the device;
3) in case where there is a suspicion that the device is in unauthorized hands the user is responsible for immediate change of all access passwords in NCU systems;
4) safety instructions of particular services may introduce additional limitations for private devices access.

§ 46

1. In case of establishing that in NCU CN a device disrupting network operation or breaching rules of this Policy is working, the proper administrator has the right to immediately deactivate access of such device to the network.
2. The administrator informs the user of the device about any cases of breaching Policy and, in justified cases or where there is lack of reaction from the user, also an appropriate superior of the user.
3. Any cases of breach of this POlicy are registered by administrators.

Chapter 9
Access passwords policy

§ 47

Administrators of central services, in order to access the servers, use two-stage authorization of access server. Second element of authorization is random number generated on the external device.

§ 48

1. Users are obliged to keep access data in secret. In particular giving own access password to an individual account to anyone is inadmissible.
2. Passwords have to meet the requirements of safety forced by systems of password change.
3. In systems where personal data is processed, specific passwords for the systems are used and password change is forced no less than once a month, unless additional mechanisms of protection are applied e.g. tokens or lists of one-time passwords.
4. At NCU, it is admissible to set a new password by a text message but the policy of a particular system management must regulate the rules of phone numbers' verification that are connected to accounts.

Chapter 10
Change of device user and disposal of electronic devices and data storage devices

§ 49

The user of the electronic device forwarded to another user and that may contain any data that require protection, is obliged to assess the risk connected with eventual share of data. If it is necessary, the user deletes data in a way which does not allow data recovery. In case of a doubt, the user contacts a proper administrator of the network.

§ 50

1. Electronic devices is under general disposing provisions adopted by NCU.
2. Collection and disposal of devices which may contain data that require protection e.g. device on which personal data was processed, may be entrusted to those entities only which have an appropriate certified authorization.
3. Devices for disposal which may contain data that require protection must be appropriately marked on the cover so that it could be forwarded to an appropriate disposing entity.

§ 51

If data storage devices containing data requiring protection did not undergo data disposal procedure, they can be entrusted to entities with a proper certificate for disposal.

§ 52

If data storage devices with data requiring protection requires warranty repair, one of the following conditions must be met.:

1) data on the storage device are encrypted;
2) data storage device cannot be entrusted to a company realising the repair, it is admissible to exchange the device with saving the original storage device by the owner.

Chapter 11
Final provisions

§ 53

1. Following orders are repealed:
   1) Order No. 144 of NCU Rector of 19 October 2009 on using professional email for professional purposes by NCU employees (NCU Legal Bulletin No. 9, item 283);
   2) Order No. 76 of NCU Rector of 18 September 2007 – Regulations for Nicolaus Copernicus University Computer Network (NCU Legal Bulletin No. 7, item 178).
2. This order shall enter into force on 19 December 2017 except § 20 - § 22 and § 24 - § 26, which enter into force on 1 July 2018

R E C T O R

prof. dr hab. Andrzej Tretyn

Appendix No. 1 to the Resolution No. 196
of the NCU Rector of 19 December 2017

Managing accounts

Creating accounts

1. NCU CN accounts of academic teachers are created at the moment of entering into employment.
2. NCU CN accounts of other employees and persons named in § 6(2) point 3, are held upon request of the person concerned, attested by the head of the home faculty or upon request of the supervisor.
3. NCU CN accounts of the doctoral students are held on the University's general server of accounts and are created independently by the concerned with the help of tools provided by the UCI.
4. NCU CN accounts of other students are held on the University's general server of accounts accordingly to the following rules:
    1. the number of student's album is an identifier of NCU's CN account;
    2. NCU's CN account is created automatically at the moment of admission to higher education studies and are activated by the student with the help of tools provided by the UCI.
    3. student's entitlements resulting from owning a NCU's CN account expire on 30 April or 30 November of the year in which the student graduated depending on the fact which of these deadlines will be earlier;
    4. the student who was removed from the list of students loses his entitlement to NCU's CN account since the date of the removal from the list.
5. NCU CN accounts of retirees and annuitants are held on the University's general server of accounts accordingly to the following rules:
    1. new accounts are created upon request of a concerned person attested by the Human Resources Department (or CM HR Department);
    2. existing accounts of employees that are retiring at the pension age or due to incapacity for work are held by the same identifier as employee account;
    3. account validity is the subject of verification accordingly to provisions in point 6 in Sustaining of accounts validity part.
6. NCU CN account for the University's guests are held upon request signed by the head of proper faculty for a limited period of time specified in the request.
7. NCU CN accounts for persons taking part in courses, apprenticeships and not encompassed with academic system of student service are created upon request attested by the Dean or Vice-dean of the home faculty.
8. Functional accounts of NCU faculties are created upon request attested by the head of the faculty.
9. Functional accounts or student and self-governing organizations as well as student research groups are created upon request attested by the Rector or a Dean for an academic year period.

Extension of account validity

1. NCU CN account created for conducting classes (§ 6(2) point 3) are renewed automatically on the basis of information provided by the University Support System of Studies (USOS).
2. Persons who own NCU CN accounts created for a specified period of time are informed via email on approaching account expiration time.
3. Validity of NCU CN accounts of students not encompassed by the system of student service is extended upon request attested by a Dean or Vice-Dean of home faculty.
4. Validity of NCU CN accounts for NCU guests is extended upon request signed by the head of the proper faculty.
5. Validity of function accounts of student and self-governing organizations as well as student research groups is extended for the next academic year after a phone or email confirmation that the account is still in use.
6. The accounts of retirees and annuitants which are not active for the period of 365 days are to be verified over the phone or via email with the owner of the account.

Blocking the accounts

1. The administrator has the right to temporarily block the account if it is improperly protected or there is a justified suspicion that the account is used by unauthorized persons.
2. The administrator unlocks the account after ensuring that the account is properly protected and is not used by third parties.

Removing of the accounts

1. NCU CN accounts of employees expire at the moment of termination of the employment. After 3-month withdrawal period invalid accounts are deleted.
2. NCU CN accounts of retirees and annuitants expire if it is established that the account is inactive its verification is impossible. After 3-month withdrawal period invalid accounts are deleted.
3. NCU CN accounts of students and doctoral students who graduated in the winter term are deleted on 30 April. The accounts of students and doctoral students who graduated in the summer term are deleted on 30 November.
4. NCU CN accounts of remaining students are deleted after they expire.
5. NCU CN accounts of guests are deleted after they expire.
6. NCU CN function accounts are deleted upon request attested by the head of the faculty.
7. NCU CN function accounts of student and self-governing organizations as well as student research groups are deleted after expiration or upon request attested by the Rector or a Dean.

Appendix No. 1 to the Resolution No. 196
of the NCU Rector of 19 December 2017

Managing domains

Creating domains

1. Names in the umk.pl domain representing faculties of NCU or projects executed at NCU are registered upon request of NCU employee. The request must be attested by the Rector, the Dean or the Head of the interfaculty or institution-wide unit. The name is registered for the period of 3 years. For subdomains maintenance a function account, owner of which is the requester, is created.
2. Names in the umk.pl domain representing student organisations or student projects executed at the NCU are registered upon request of NCU employee or student.The request must be attested by the Rector or the Dean. The name is registered for the period of full academic year. For subdomains maintenance a function account, owner of which is the requester, is created.
3. Names representing individual activity of NCU employees are registered in the prac.umk.pl domain upon request of NCU employee made over the phone or via email. For subdomains maintenance the personal NCU CN account of the employee is used.

Deleting domains

1. At the moment of expiration of domain validity or lose of account validity provided for the domain maintenance, the verification procedure is applied in order to examine whether the domain is still necessary and if the owner is still to be responsible for it. In case of establishing that the domain should be deleted, NCU CN administrator sends the notification to a proper function person (the Rector, the Dean etc. depending on who attested the first request for the domain).
2. The names in prac.umk.pl domain are checked out at the moment of a validity loss of NCU CN employee account.

Appendix No. 3
of the NCU Rector's Regulation No 196 of 19 December 2017

Terms and conditions of the external network services usage available via Central Authentication Service

§1

NCU IT Center (UCI) in cooperation with Polish Identity Federation PIONIER.Id allows access to external network services. Logging in is made via NCU Central Authentication Service through NCU account.

§2

The user is obliged to maintain logging safety by abiding by the document ***Zalecenia dotyczące bezpiecznego logowania*** *(Recommendations for secured logging)* available on the UCI websites.

§3

1. During the logging in to external service process providing selected data regarding user account such as e-mail address, status (employee or student), surname and name is usually necessary.
2. Before sending the data the user is asked for permission which may be provided once or permanently.
3. Before logging in to the service the user may check Privacy Policy regarding this particular service.

§4

1. Unless provided otherwise, the user may use the service only for his/her needs related to his/her status at NCU, that is work or studies at NCU.
2. The user must comply with eventual additional restrictions described on service pages, e.g. large-scale data downloading prohibition or unauthorized data publication etc.
3. The user may not share own account with other persons.
4. The user may not run the software using the service on his/her behalf.