Annexe to Order No. 2 of the Rector of Gdynia Maritime University of 24 January 2022

Gdynia Maritime University Computer Network Regulations

I. Nature of the GMU CN

Section 1

The Gdynia Maritime University Computer Network, hereinafter referred to as the GMU CN, operates within the framework of the Tri-City Academic Computer Network (TASK) and is subject to the provisions contained in the *Regulamin Trójmiejskiej Akademickiej Sieci Komputerowej TASK* (Regulations of the Tri-City Academic Computer Network TASK).

Section 2

The purpose of the GMU CN is to provide Internet access for the scientific and educational needs of the University. The GMU CN is a campus network comprising technical and software resources that connect the individual local GMU networks by means of access and distribution telecommunications nodes and a central node. The task of the GMU CN is to provide services available through the network at a level resulting from its current software and technical capabilities. The recipients of GMU CN network services are employees and students of Gdynia Maritime University.

Section 3

The computer network or its subnet is assigned to an organisational unit referred to as the Central Operator of the GMU CN (hereinafter referred to as the Central Operator). The Central Operator is responsible for managing the network or subnet through its administration, operation and development.

Section 4

The GMU CN is a multi-protocol network. The basic network protocol is TCP/IP, and the physical layer is Ethernet II. Operation using other network protocols is also permitted. Operation using protocols other than TCP/IP may be carried out only with the consent of the Central Operator.

II. Structure and Operation of the GMU CN

Section 5

1. The Central Operator is the Computer Networks Section of the IT Technicians Team (hereinafter referred to as the Computer Networks Section), which reports to and is supervised by the Head of the IT Technicians Team.
2. The Computer Networks Section of the IT Technicians Team comprises:
   1) the central administrator;
   2) the network administrator;
   3) the network engineer.

Section 6

1. As the Central Operator, the Computer Networks Section is responsible for managing the GMU CN (development, administration and operation), and in particular for:
   1) initiating network development;
   2) developing and implementing IT projects for the development of the GMU CN;
   3) managing GMU CN resources assigned to the IT Technicians Team;
   4) supervising the proper operation of the network;
   5) supervising and administering the central node (implementing the network core layer) and dedicated telecommunications nodes (implementing the distribution and access layers of the network);
   6) operating, maintaining and configuring the core, distribution and access network devices assigned to the IT Technicians Team;
   7) administering network resources, i.e., assigning addresses, names, passwords, masks, permissions, access modes, etc.;
   8) assigning internet numbers and addresses within the numbering range allocated by the TASK IT Centre (CI TASK);
   9) ensuring network security in accordance with GMU's security policy;
   10) administering (supervising, operating and modernising) the services specified in Annexe 1 (List of Services Managed by the GMU CN);
   11) developing the range of available services;
   12) ensuring continuous access to the GMU CN subnets.
2. The Central Operator may delegate part of its powers relating to node management to local administrators of GMU CN local networks, provided that this is accompanied by a detailed specification of the rights and responsibilities of the local administrator assuming those powers, together with the designation by name of the person responsible and prepared to perform this task.

Section 7

The GMU CN comprises three locations:

1. GMU1 – the complex of buildings on Morska Street, including the following subnets:
   a) the Faculty of Electrical Engineering,
   b) the Faculty of Marine Engineering,
   c) the Faculty of Management and Quality Science,
   d) the Rector's Office,
   e) the Deputy-Rectors' Offices,
   f) the Main Library,
   g) the Finance Office,
   h) Student Residences Nos. 3 and 4;
1. GMU2 – the complex of buildings on Aleja Jana Pawła II and F. Sędzickiego Street, including the following subnets:
   a) the Faculty of Navigation,
   b) Student Residence No. 2;
1. GMU3 – the premises of the Maritime Institute located in Gdańsk, including the following subnet:
   a) the Maritime Institute.

All GMU CN locations – GMU CN1, GMU CN2 and GMU CN3 – are connected to the Tri-City Academic Computer Network TASK.

Section 8

3. Within the GMU CN, the following subnets are distinguished:
   1) the Main Library subnet (PBG);
   2) the Faculty of Electrical Engineering subnet (PWE);
   3) the Faculty of Marine Engineering subnet (PWM);
   4) the Faculty of Navigation subnet (PWN);
   5) the Faculty of Management and Quality Science subnet (PWZNJ);
   6) the Rector's Office subnet (PR);
   7) the Vice-Rectors' Offices subnet (PPR);
   8) the Maritime Institute subnet (PIM);
   9) the Finance Office subnet (PK);
   10) the subnets of Student Residence Halls Nos. 2, 3 and 4 (PSDM2, PSDM3 and PSDM4); the Eduroam wireless access subnet (PER).
4. Each of the above subnets may comprise a number of local subnets. The operators of these subnets are:
   1) the Faculties (subnets PWE, PWM, PWN, PWZNJ);
   2) the Main Library (subnet PBG);
   3) the Maritime Institute (subnet PIM);
   4) the Finance Office (subnet PK);
   5) the Computer Networks Section of the IT Technicians Team (subnets PSDM2, PSDM3, PSDM4, PER, PR, PPR).
5. Each local subnet may be administered by employees of the above GMU units acting as a local network (subnet) administrator, responsible for subnet management (development, administration and operation).
6. The method of appointment, the detailed scope of responsibilities, and the form of employment of staff acting as local network administrators shall be determined by the operator of the relevant subnet.
7. The responsibilities of the local network administrator include:
   1) direct cooperation with the Central Operator in matters concerning the operation of subnet nodes;
   2) informing the Central Operator of all events relating to the operation of nodes that may affect their functioning (e.g., planned power shutdowns);
   3) taking care of the network equipment installed in the nodes;
   4) supervising the proper power supply of the nodes;
   5) protecting the nodes against unauthorised access;
   6) strictly maintaining the confidentiality of entrusted information concerning the nodes;
   7) ensuring and maintaining the confidentiality of information transmitted over the network;
   8) ensuring the Central Operator has unrestricted access to the nodes;
   9) participating in training organised by the Central Operator;
   10) performing activities connected with the powers delegated by the Central Operator.

Section 9

1. The operation of the GMU CN computer network is implemented by means of the University Network Backbone, consisting of passive and active parts located on the GMU campus (dedicated rooms and telecommunications shafts).
2. The University Network Backbone consists of:
   1) a central node (core layer) equipped with:
      a) network devices, servers, storage arrays, power backup UPS units, passive components, optical and electrical transmission media;
      b) software dedicated to standard network services installed on appropriate devices;
      c) software for University-wide applications installed on appropriate devices;
      d) passive fibre-optic and UTP patch panels;
   2) dedicated telecommunications nodes (distribution and access layers), usually equipped with:
      a) network devices, servers, UPS units with power backup, passive components, optical and electrical transmission media;
      b) passive fibre-optic patch panels used for connections with the network core layer;
      c) passive UTP patch panels used to connect users of local operators' subnets or local nodes;
      d) passive fibre-optic patch panels used to connect local operators' subnets or local nodes;
   3) fibre-optic cabling connecting the telecommunications nodes (access and distribution layers) with the central node (network core layer), laid in appropriate vertical telecommunications shafts in buildings and horizontal shafts on the GMU site.
3. The operation and expansion of the University Network Backbone are financed from University funds, grants and dedicated external subsidies. The University Network Backbone is managed by the Central Operator.
4. The Central Operator has the exclusive right to modify the University Network Backbone infrastructure (i.e., equipment type, cabling and software).
5. The local operators' subnets are connected to the University Network Backbone at the telecommunications nodes. These subnets consist of:
   1) transmission media;
   2) PC workstations and other devices;
   3) local servers together with software;
   4) end-user access devices (routers, switches, access points).
6. Connecting a subnet to the University Network Backbone and any modernisation of it always requires the knowledge and consent of the Central Operator.
7. The operation and expansion of a subnet are financed from the funds of the local operator (the relevant unit).

Section 10

1. Equipment of local network nodes may be recorded as assets of the organisational unit designated by the relevant network or subnet operator. The ownership of equipment (switches, routers, etc.) by a given unit is determined by its appropriate inventory number.

2. Equipment of the central node (together with the central network servers and storage arrays) and dedicated telecommunications nodes (including active network devices or servers) is recorded as assets of the IT Technicians Team.
3. Placement of a subnet operator's device in dedicated telecommunications nodes requires the consent of the Central Operator. This requires prior arrangements and compliance with relevant requirements by the subnet operator.

Section 11

1. The environment of the GMU CN that is relevant to its operation also includes the so-called operational utilities (dedicated electrical power supply, air conditioning), which are under the responsibility of the Chancellor of GMU. The requirements for operational utilities (their type, parameters, etc.) are specified by the Central Operator and by subnet operators.
2. Financing (development and operation) of operational utilities is provided from:
    1. University funds – in relation to the central node and dedicated telecommunications nodes;
    2. subnet operators' funds – in relation to subnets and local nodes.

Section 12

1. The Central Operator exercises its powers in relation to the entire GMU CN. Subnet administrators exercise their powers in relation to their respective subnets and are responsible for ensuring that the actual state of the subnet corresponds to the state registered by the Central Administrator.
2. If disruptions occur in the operation of a subnet, the Central Operator has the right to disconnect that subnet. This requires notifying the operator of the subnet from which the disruptions originated.

Section 13

1. A new subnet may be connected to the GMU CN with the consent of the Central Operator, after approval of the submitted subnet design, agreement on the technical conditions to be met by network devices and computer stations, and verification that the implementation complies with the approved design.
2. The Central Operator has the right to refuse connection of a local network to the GMU CN if it does not meet the technical norms and network standards adopted for the GMU CN (this applies both to hardware and software), or if it has been implemented inconsistently with the approved design. This also applies to any extension, any change of hardware and software, and any change in subnet topology.

Section 14

It is prohibited to perform any activities that may disrupt the functioning of the GMU CN without the approval of the Central Operator. Such activities include, in particular: changing device configuration without the administrator's knowledge and consent, disconnecting cabling, replacing network equipment, changing network software or its configuration, and connecting unregistered devices to the network without the administrator's knowledge and consent.

III. Rules for Using the GMU CN

Section 15

A user of the GMU CN is any person using network services under an appropriate agreement with GMU. User status is granted to employees, students and persons participating in research conducted by GMU or cooperating with GMU. Operators of other academic and research institutions may also be users of the GMU CN, subject to the Rector's consent.

Authorisations to use services available on the GMU CN are granted and withdrawn, at the request of authorised persons and with the consent of heads of organisational units, by the relevant subnet administrators. A person holding the status of GMU student receives user rights for the period of their studies (including Dean's leave or medical leave). The Central Operator also has the right to grant user authorisations.

Section 16

1. Unauthorised access to GMU CN resources (using other users' passwords, disclosing passwords, monitoring network traffic, etc.) results in disciplinary and legal consequences.
2. Loss of user status as a result of termination of an employment contract (or other agreement), or loss of student status, results in loss of the granted user status. An employee or student settling their affairs with the University must obtain a note from the subnet administrator or the central administrator on the relevant document.
3. The owner of a computer (computer system, network station (host), server, database, information system) is its administrator. The administrator bears full responsibility for the security and IT condition (compliance with IT standards) and the manner of use of the computer (i.e., hardware, software and data).

Section 17

1. Users of the GMU CN retain the right to the inviolability of their personal rights (protection of the confidentiality of correspondence, personal data, etc.) in connection with the services provided. Network/subnet administrators and computer/service administrators having access to other users' data are obliged to observe professional secrecy. Network/subnet and computer administrators are not responsible for breaches of personal rights caused by other users (e.g., disclosing a password to third parties).
2. Any actions aimed at obtaining unauthorised access to GMU computer resources are prohibited, in particular, impersonating other users or monitoring GMU CN links. If such actions are detected, the network/subnet administrator has the right to block the user's access rights and is simultaneously obliged to notify the superiors of the user's improper conduct.

Section 18

1. It is permissible, subject to the consent of the relevant administrator, to create publicly accessible information systems operating on computers connected to the GMU CN. The administrators of such systems are responsible for their proper functioning.
2. Making one's own (private) information resources available via the GMU CN (e.g., a website, mail server, FTP, etc.) requires the prior consent of the Central Operator or subnet operators in each case.

Section 19

If it is found that the GMU CN infrastructure is being used for a purpose other than that set out in Section 2, the Central Operator shall notify the Rector of GMU of the situation.

Section 20

1. Administrators of computers/systems connected to the GMU CN are obliged to inform users of any suspicion of unauthorised use of those computers/systems and of any problems connected with their operation.
2. Users of the GMU CN are obliged to comply with the recommendations of computer/system administrators in matters concerning the security or efficient operation of those computers.

Section 21

The Central Operator may maintain Internet connection billing records where such a need is reported (e.g., for the purposes of settling grants or projects).

Section 22

Every user of the GMU CN is obliged to familiarise themselves with these Regulations. Users who breach the Regulations of the GMU CN shall bear disciplinary or criminal liability.

Annexe 1 – List of services managed by the GMU CN

The services managed by the GMU CN are:

1. the DNS (Domain Name Service) for network servers and devices, and for computers operating in the GMU network;
2. the DHCP service;
3. the email service on GMU servers and in the Microsoft365 cloud;
4. the free Microsoft365 A1 service – a set of applications and services available in the public cloud on Microsoft servers (the most important of which include Microsoft365/Exchange cloud email, the OneDrive network drive, Teams video conferencing, and SharePoint) (the rules and access to this service are governed by Annexe 3);
5. the academic and educational access service to the Internet:
   a) wired access via the GMU CN infrastructure;
   b) Eduroam wireless access via the GMU CN infrastructure and the PIONIER network (the rules and access to this service are governed by Annexe 2);
6. the moderated VPN access service to applications operated within the GMU campus;

7. access to external network services through the GMU Central Login Point, using a GMU account in cooperation with the PIONIER.Id Polish Identity Federation (the rules and access to this service are governed by Annexe 4).

Annexe 2 – Regulations of the Eduroam service

Section 1

The Eduroam service (Education Roaming) is provided on the campus of Gdynia Maritime University (GMU) – a network enabling secure roaming for users of scientific and higher-education institutions.

Section 2

Use of Eduroam resources is equivalent to acceptance of the Eduroam Service Regulations available at: http://www.eduroam.pl/regulamin and of the Gdynia Maritime University Computer Network Regulations.

Section 3

The service may be used by employees and students of GMU, as well as by users of other universities who have Eduroam user status at their home institution.

Section 4

Eduroam access is granted to a GMU employee or student who:

1. completes the user registration/verification stage in the CUI system: https://cui.umg.edu.pl
2. activates the Eduroam service by completing and accepting the relevant form from the My Services menu entitled: Eduroam Service Activation.

Section 5

1. Eduroam access for a GMU employee or student ends upon:
   1) completion of studies by the GMU student;
   2) loss of GMU student status;
   3) termination of the GMU employee's employment contract.
2. A user may not make their Eduroam account available to other persons.

Section 6

Gdynia Maritime University bears no responsibility whatsoever for any costs or penalties imposed on network users resulting from breaches of these Regulations or of applicable legal provisions (in particular infringement of copyright), or from the dissemination over the network of content infringing legal or moral standards, or the rights and good name of other users or third parties/persons/companies.

Section 7

1. A breach of the provisions referred to in Section 2 may result in suspension of access to the Online Service in whole or in part by IT Technicians Team administrators and Microsoft.
2. The user's Online Service access within Microsoft365/A1 may also be suspended at the request of:

1) the Rector of the University;
2) the relevant disciplinary committee;
3) the relevant law enforcement bodies and courts.

Section 8

Information concerning the Eduroam service (registration, technical requirements, security policy) is available at: https://eduroam.umg.edu.pl

Annexe 3 – Regulations of the Microsoft365 service

Section 1

These Regulations govern the use of the free online applications and services of Microsoft365 A1 for Education, hereinafter referred to as the Microsoft365 Regulations.

Section 2

For the purposes of these Regulations:

1. GMU means Gdynia Maritime University;
2. Microsoft means the producer of the Microsoft Windows operating systems and Microsoft Office/Microsoft365 cloud office software;
3. Microsoft365 means the Microsoft365 A1 service plan (free online access to the relevant services and applications) available at: https://products.office.com/pl-pl/academic/compare-office-365-education-plans;
4. CUI means the Internet Services Centre, the University web application whose task is to verify the identity of a user applying for access to services on the basis of the University's internal systems and to activate the service;
5. IT Technicians Team means the organisational unit of GMU;
6. CN means the Computer Network at Gdynia Maritime University;
7. Microsoft Azure AD means the Active Directory service in the Microsoft Azure cloud for GMU domains and subdomains, managed by the IT Technicians Team;
8. Official Account means an account used by a staff member employed under a contract of employment for official purposes (scientific development, teaching, administrative work for the University), and who is obliged to comply with GMU's Security Policy when using the functionalities connected with the assigned services and applications.
9. Educational Account means an account used by a GMU student for education and academic development during their studies, and who is obliged to comply with GMU's Security Policy when using the functionalities connected with the assigned services and applications.

Section 3

1. Microsoft365 A1 is a free online version of the Microsoft Office suite, offering functionalities such as email (email address), video conferencing, the standard Word, Excel and PowerPoint applications, contacts, and OneDrive storage space.
2. A detailed description of the Microsoft365 A1 applications and services is available at: https://www.microsoft.com/pl-pl/microsoft-365/academic/compare-office-365education-plans?activetab=tab%3aprimaryr1 under the Microsoft 365 A1 plan tab.

Section 4

The rules for using Online Services within Microsoft365 and the obligations relating to the processing and protection of user data and personal data by Online Services are set out in Microsoft documentation:

Document Title	URL
Online Services Team	http://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=OST&lang=Polish
Microsoft Services Agreement, MSA	https://www.microsoft.com/pl-pl/servicesagreement/
Microsoft Services Agreement Supplement MICROSOFT OFFICE 365 CONSUMER SUBSCRIPTION ON SERVICE AND SOFTWARE	https://www.microsoft.com/en-us/Useterms/Retail/Microsoft365/University/Useterms_Retail_Microsoft365_University_Polish.htm
Privacy Statement	https://privacy.microsoft.com/pl-pl/privacystatement

Microsoft Online Subscription Agreement	https://azure.microsoft.com/pl-pl/support/legal/subscriptionagreement/

Section 5

1. Persons entitled to use the Microsoft365 service are:
   1) persons holding current GMU student status;
   2) persons employed by GMU.
2. User account names for the Microsoft365 service are created according to the following rules:
   1) Students – the student's Educational Account is created according to the following format: student_record_number@student.umg.edu.pl
   2) Employees – the employee's Official Account is created according to the following format: initial.surname@[subdomain].umg.edu.pl
3. Functional account names are not accepted.

Section 6

Access is granted to a user who:

1. meets the criteria referred to in Section 5;
2. successfully completes the user registration/verification stage through the CUI system: https://cui.umg.edu.pl
3. activates the Microsoft365 service by completing and accepting the relevant form from the My Services menu entitled: Microsoft365 Service Activation.

Section 7

1. Access to Microsoft365 ends upon:
   1) completion of studies by the GMU student;
   2) loss of GMU student status;
   3) cessation of employment with GMU.
2. Resources of an employee's Official Account (folders, documents, email threads, contacts, etc.) may be transferred to another employee of the unit at the request of the head of the relevant organisational unit of GMU.
3. Resources (folders, documents, email threads, contacts, etc.) generated by a user in the Microsoft365 cloud for whom the right of access to Microsoft365 has ceased shall be physically deleted from the cloud resources after 12 months.

Section 8

1. Microsoft365/A1 is used via an Internet browser. Access to Microsoft365 is obtained after authentication in Microsoft Azure AD by entering, at the URL https://www.office.com, the relevant user name (full email address) and password.
2. The applications and services made available under Microsoft365 may be used only by a user who meets the conditions set out in Section 5 of these Regulations.

3. Authorised Microsoft365 users may use the Online Services and related software only in the manner specified in the volume licensing agreement concluded by the University, for which Microsoft reserves all other rights.
4. Users may not use the Microsoft365 service:
    1. in a manner inconsistent with statutory or subordinate legislation;
    2. in a manner infringing the rights of other persons;
    3. in order to obtain unauthorised access to other services, devices, data, accounts or networks, or to disrupt their operation;
    4. in order to send spam or distribute malicious software;
    5. in a manner that may be harmful to the Online Service or disrupt its use by other persons;
    6. for any purpose or in any situation where failure or malfunction of the Online Service could lead to death, serious bodily injury, serious physical damage or serious environmental pollution.
5. A breach of the provisions contained in Section 8(4) may result in suspension of access to the Online Service in whole or in part by administrators of the IT Technicians Team and by Microsoft.
6. The user's Online Service access within Microsoft365/A1 may also be suspended at the request of:
    1. the Rector of the University;
    2. the relevant disciplinary committee;
    3. the relevant law enforcement bodies and the courts.

Section 9

Any application or service of Microsoft365 activated on an online-access basis is covered by the Microsoft manufacturer's warranty, in accordance with the terms set out in the Microsoft licence.

Section 10

Microsoft365 complies with international protection standards, as confirmed by the ISO/IEC 27001:2005 certificate. The service is also subject to regular audits. It also holds an ISO 27018 certificate confirming compliance of its services with cloud personal data protection standards, which means that customer data stored in the cloud will not be used for marketing purposes without their knowledge.

Section 11

In matters not regulated by these Regulations, the GMU Computer Network Regulations, GMU's Security Policy, and the manufacturer's licence – Microsoft Agreement: https://azure.microsoft.com/pl-pl/support/legal/subscription-agreement/ shall apply.

Annexe 4 – Regulations for the use of external network services available through the Central Login Point

Section 1

The IT Technicians Team of Gdynia Maritime University, in cooperation with the PIONIER.Id Polish Identity Federation, provides access to external network services. Logging into such services is carried out through the GMU Central Login Point, using a GMU account.

Section 2

The user is obliged to ensure login security by following generally accepted principles of secure use of IT systems.

Section 3

1. When logging into an external service, it is usually necessary to transfer selected data relating to the user's account, such as surname, first name, University email address, and status within GMU (employee or student).
2. By logging into an external service, the user thereby consents to the transfer of their data to the relevant Service Provider. Giving such consent is voluntary, but necessary for the user to log into the external service successfully.
3. Users' personal data are processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as the GDPR.
4. GMU informs the user that, in connection with logging into an external service, the user's personal data will be transferred to the Service Provider for the entire period of GMU's membership in the PIONIER.Id Polish Identity Federation, but no longer than until the user loses the status referred to in Section 3(1).
5. Before logging into a service, the user may check the Privacy Policy relating to that service.

Section 4

1. Unless the regulations of a given service provide otherwise, the user may use the service solely for their own needs connected with their status at GMU, i.e., work or studies at GMU.
2. The user must comply with any additional restrictions described on the service websites, for example, a prohibition on mass downloading of data or its unauthorised publication.
3. The user may not make their own account available to other persons.
4. The user may not run software that uses the service on their behalf.