REGULATION
ON THE PROCESSING OF INFORMATION CONTAINING PERSONAL DATA IN THE "HUMAN RESOURCES" SYSTEM (EMPLOYEE RECORDS)

I. GENERAL PROVISIONS

1.1. The Regulation on the processing of information containing personal data in the University Management Information System "Human Resources" (hereinafter "Regulation") is developed in order to implement within the Public Institution Technical University of Moldova (hereinafter TUM) the provisions of Law no. 133 of 8 July, 2011 "On the protection of personal data", and of the "Requirements regarding the ensuring the security of personal data when processing personal data within personal data information systems", approved by Decision 1123 of December 14, 2010, and in compliance with the provisions of Art. 91 - 94 of the Labor Code of the Republic of Moldova.

1.2. This Regulation governs the general conditions and requirements for processing of personal data of UTM employees within the framework of the Management Information System "Human Resources" (hereinafter - SIMU "Human Resources").

II. SCOPE

2.1. Purpose of processing information containing personal data in EMIS "Human Resources" is to ensure the recording of information relating to recruitment, employment, the execution of the terms of individual employment contracts, retirement as well as the submission of quarterly and annual reports to the institutions state institutions, according to the legislation in force.
2.2. The following categories of data are processed within SIMU "Human Resources" personal data:

- first name, last name;
- sex;
- date and place of birth;
- citizenship;
- IDNP
- picture;
- family situation;
- military situation;
- personal data of family members;
- your driving license;
- data for the transfer to the bank account of salary payments and other amounts due as allowances, compensation or other benefits, as the case may be;
- signature;
- civil status records;
- personal social insurance code (CPAS);
- health insurance code (CPAM);
- phone/fax number;
- mobile phone number;
- address (home/residence);
- e-mail address;
- profession and/or occupation;
- vocational training - diplomas - studies;

- name, surname, forenames (patronymic, if applicable) of the people responsible for person's dependents (family members, other relatives and people, as the case may be);
- the actual amount of calculated salary entitlements, taxes and duties including compulsory social security contributions for social assistance health and social security contributions, and other amounts due by virtue of law or contract;
- data from certificates of sick leave granted, necessary for calculation of the corresponding allowance;
- where appropriate, other data necessary for the fulfillment of that purpose in accordance with legislation in force.

2.3. The processing of personal data referred to will be carried out for fulfill the following purposes:

a) Processing of information on changes in the processing of personal data personal data concerning employees which have an impact on the performance of the individual employment contract;
b) Establishment of the staff salary system in accordance with the legislation in force of the Republic of Moldova;
c) Processing employees' sick leave certificates in order to establish corresponding allowances;
d) Drafting, recording and processing of the Rector's personnel orders;
e) Submission to the CNAM of the nominal register of new and dismissed employees, in paper and electronic format;
f) Registering and processing applications for competitions to fill vacant posts;
g) Drawing up the REV 1 insured person declaration for each employee and their transmission to the Territorial House of Social Insurance, the Buiucani branch on support paper;
h) Assisting the process (by providing the necessary information) for completing periodic (monthly) reporting and reporting on the income paid and the income tax paid income retained;
i) Completion of monthly, quarterly and annual statistical reports on TUM staff;
j) Processing applications and documents necessary for the performance of individual employment contracts;
k) Keeping employees' personal files;
l) Recording data in workbooks;
m) Other purposes, necessary for the performance of human resources management activities.

2.4. Personal data covered by this Regulation will be stored by the people responsible within UTM in such a way as to allow identification of data subjects strictly for the period necessary to achieve the purposes for which the data are processed, and on expiry of that period, the records will be destroyed/ deleted, depending on depending on the medium on which they were made. In the case of obligations expressly laid down by law, they may remain in storage with archive document status.

2.5. Any use of personal data entered in SIMU "Human Resources" for purposes other than those mentioned above is prohibited.

III. GENERAL CONDITIONS FOR ENTERING INFORMATION IN THE REGISTER

3.1. Personal data contained in the SIMU "Human Resources" within UTM shall be processed and stored:

1. on paper;
2. in electronic format:
   a) Software - SIMU "Human Resources", which is installed on all computers employees of the Human Resources Service;
   b) Hardware - computers, which are located in the offices of the Service's employees Human Resources - in the central building of TUM, located at: Chisinau municipality, 168 Stefan cel Mare and Saint blvd.

3.2. The maintenance of the record-keeping software is performed by the employees of the Service Design and Development of Information Systems and Software Products of the Information Technology and Communications Directorate of TUM, with the following tasks:

- Making adjustments in the program based on changes in the legislation of the Republic of Moldova;
- Eliminate errors in program operation;
- Consulting in resolving difficulties in using the program;
- Examination of requests received from the Human Resources and Economic Planning;
- Review of the Human Resources and Economic Planning Service database;
- Review and non-disclosure of information with limited accessibility that has become known when providing these services.

3.3 The processing of information in SIMU "Human Resources" on paper is structured according to the "folders-folders" criterion, being kept in filing cabinets, which are located physically located in the Human Resources Service office at UTM headquarters.

IV. STORAGE DURATION

4.1. The processing of personal data in SIMU "Human Resources" is carried out during the period of activity of the MTU employees (from the moment of signing the individual contract employment until the completion of the actions provided for by the legislative acts in case of termination of employment). After termination of employment, the files employees are kept at the Human Resources Service for 3 years from the date of termination of employment. employment relationship.

4.2. On expiry of the deadlines referred to in point 4.1, the data in SIMU "Resources shall be kept in archived form for the period established by the General *Nomenclature of TUM files, approved by the Rector on 17.03.2016*, thereafter they are subject to destruction or deletion, depending on the medium on which they were made.

V. RIGHTS OF EMPLOYEES AND DATA SUBJECTS

5.1. TUM, as a personal data controller, ensures that the personal data protection rights of its employees and, where applicable, other data subjects are respected.

5.2. In accordance with the principles of personal data protection, data subjects have the following rights: the right to information, the right of access to data, the right to intervene, the right to object to personal data concerning them and the right to have recourse to the courts.

5.3 All people involved in the administration and/or processing of information from SIMU "Human Resources" shall comply with the procedure for access to data personal data.

5.4. Employees' right of access to information concerning them shall be granted only upon express written request, with the direct consent of the Rector of UTM. The information provided will be granted in such a way as not to prejudice the rights of third parties. People requesting personal data must indicate the purpose of the request, as well as the specific period for which they require the information.
5.5. The right of access may be refused where the exceptions provided by law apply. The need to restrict access may arise where there is an obligation to protect the rights and freedom of third people, such as for example, if other people are included in the information requested and there is no possibility to obtain their consent, or it is not possible to extract, by editing, the irrelevant personal data.

VI. MEASURES FOR THE PROTECTION OF PERSONAL DATA PROCESSED IN THE HUMAN RESOURCES SIMU

6.1. General information security management measures
6.1.1. In case of temporary non-utilization of paper or electronic information carriers containing data retrieved from EMIS Human Resources, they shall be kept in locked safes.
6.1.2. At the end of work sessions, computers and printers are disconnected from the mains.
6.1.3. The operator shall ensure the security of points of receipt and dispatch of mail as well as security against unauthorized access to the machines copying machines.
6.1.4. Physical access to the means of representation of information retrieved from SIMU "Human Resources" is blocked against viewing by unauthorized people.
6.1.5. Means of processing information retrieved from the Human Resources MIS or software intended to process them shall be removed from the security perimeter only with the written permission of the controller.
6.1.6 Removal and insertion of information processing means from the SIMU 'Human Resources' from/within the security perimeter shall be recorded in the register.
6.2. Measures for the protection of personal data processed in the SIMU "Resources Human Resources, shall be carried out taking into account the need to ensure confidentiality and integrity, through protection in manual, electronic and external form.
6.3. Special marking requirements: all information output from the SIMU "Resources containing personal data shall be subject to marking, indicating prescriptions for further processing and dissemination, including the indication of the unique identification number of the personal data controller.
6.4. The office is never left unattended when going outside, the office door is kept locked.
6.5. Before granting physical access to the Human Resources MIS, the following shall be verified access competences.
6.6. Monitoring registers shall be kept for a minimum of one year. the specified period, they shall be liquidated and the data and documents contained in the register subject to shall be transferred to the archives.
6.7. The security perimeter is considered to be the perimeter of the office in which SIMU 'Human Resources' is located and physically intact.
6.8. Computers are located in areas with restricted access for outsiders.
6.9. Doors and windows are locked in the absence of employees in the room authorized to administer the system.
6.10. The location of the SIMU "Human Resources" responds to the need to ensure security against unsanctioned access, theft, fire and other possible risks.
6.11. Electrical safety: the safety of the electrical equipment used to maintain the functionality of the SIMU "Human Resources", of the electrical cables, including their protection against damage and unsanctioned connections, is ensured. In the event of an

exceptional situation, breakdown or force majeure, the possibility of disconnecting the electricity to the SIMU 'Human Resources', including the possibility of disconnecting any ICT component, is ensured.

6.12. The computers, where the SIMU "Human Resources" is physically located, are equipped with UPSs, which are used for the correct termination of the working session of the systems (components) in case of disconnection from the power supply.

6.13. Network cable security: the network cables, through which data transmission operations retrieved from the SIMU Human Resources are protected against unsanctioned connections or damage. To exclude jamming, voltage cables are separated from communication cables.

6.14. SIMU "Human Resources" fire safety: the office where it is located SIMU "Human Resources" is equipped with fire safety equipment and meets the requirements and fire safety standards in force.

6.15. Control of the installation and removal of ICT components: control and record of the installation and removal of program, technical and technical program means, used within the SIMU "Human Resources". At the expiry of the retention period, the information, containing personal data, on information carriers, shall be destroyed.

VII. USER IDENTIFICATION AND AUTHENTICATION SIMU "HUMAN RESOURCES"

7.1. The identification and authentication of users of information retrieved from UMIS "Human Resources" and the processes executed on behalf of these users.

7.2. All users (including staff maintaining system modules) have a personal identifier (User ID).

7.3. Passwords are used to confirm the user ID. The use of passwords in the process of ensuring information security: in addition to the requirements for keeping passwords confidential, it is forbidden to write passwords on paper, except in the case of ensuring the security of their safekeeping (placing the entries in a safe). At the time of entry, passwords are not clearly reflected on the monitor.

7.4. Change passwords whenever there is any indication that the system or password has been compromised.

7.5. In order to ensure that each user can be held accountable, individual user identifiers and passwords are used. The possibility for users to choose and change their individual passwords, including the possibility to activate the procedure for keeping track of their incorrect entries, shall be ensured. After three failed authentication attempts, access is blocked automatically.

7.6. In the event of termination, suspension or modification of the user's employment relationship and, as a result, the new tasks do not require access to personal data, as well as in the event of modification of the user's access rights, abuse by the user of access authorizations received for the purpose of committing a harmful act, absence of the user from the workplace for a long period (more than 2 months), the identification and authentication codes shall be revoked or suspended.

7.7. It is carried out, by automated means of support, the administration of access of users who process personal data in the UMIS Human Resources, including their creation, activation, modification, revision, deactivation and deletion. The access accounts of temporary users processing personal data registered in the UMIS Human Resources shall automatically cease to be active upon expiry of the period of time set (for each type of access account). Access accounts of non-active users processing information in UMIS Human Resources shall be automatically deactivated after a period of maximum 1/month/month.

Automated means of recording and informing about the creation, modification, deactivation and termination of action of access accounts are used.

7.8. In order to detect and avoid the granting of unauthorized access rights, the access rights of users to the UMIS "Human Resources" shall be reviewed regularly, every two months at most and after any change of user status.

7.9. The use of wireless technologies, mobile equipment is authorized by responsible people.

7.10. Limits are imposed on who is entitled:

a) view the information stored in the UMIS Human Resources;

b) copy, download, delete or modify any stored information.

7.11. All employees with access rights receive initial training in personal data protection.

7.12. Any activity of disclosing personal data to third parties shall be documented and subject to a rigorous prior analysis of the purpose and legal basis of the intended disclosure of a given volume of personal data.

7.13. Any breach of security with regard to the UMIS "Human Resources" is subject to documentation and the person responsible for implementing the security policy is informed about it as soon as possible.

7.14. Before granting access to the system, users are informed that the use of the SIMU "Human Resources" is controlled and that their unauthorized use is sanctioned in accordance with civil, contravention and criminal legislation.

VIII. SECURITY ASSESSMENT IN THE UMIS HUMAN RESOURCES

8.1. Organize the generation of security audit records in UMIS 'Human Resources' for the events, indicated in the corresponding list, subject to audit.

8.2. The user's login/logout attempts are logged according to the following parameters:

a) date and time of attempted entry/exit;

b) user ID;

c) the result of the entry/exit attempt.

8.3. The registration of the attempts to start/terminate the working session of the application programs and processes, intended for processing the information from the UMIS "Human Resources", the registration of the changes of the users' access rights and the status of the access objects according to the following parameters is performed:

a) date and time of the start attempt;

b) name/identifier of the application program or process;

c) user ID;

d) the result of the startup attempt.

8.4. The registration of attempts to obtain access (to execute operations) to applications and processes intended for information processing in UMIS "Human Resources" shall be performed according to the following parameters:

a) date and time of the access attempt (execution of the operation);

b) name (identifier) of the application or process;

c) user ID;

d) protected resource specifications (identifier, logical name, file name, number, etc.);

e) type of operation requested (read, write, delete, etc.);

f) the result of the attempt to gain access (execution of the operation).

8.5. The registration of changes in user access rights (competences) and status of access objects is performed according to the following parameters:

a) date and time of the change of competence;

b) ID of the administrator who made the changes;

c) User ID and the user's credentials or specifying access objects and their new status.

8.6. The registration of the exit from the Human Resources MIS, the registration of changes in the access rights of the subjects and the status of the access objects shall be performed according to the following parameters:

a) date and time of release;

b) the name of the information and how to access it;

c) specification of the equipment (device) that released the information (logical name);

d) user ID who requested the information;

e) the volume of the document issued (number of pages, tabs, copies) and the result of the issue.

8.7. The cases of failure of the security audit in the UMIS "Human Resources" or the completion of the entire volume of memory allocated for storing the audit results, are brought to the attention of the person responsible for the personal data security policy, who takes measures to restore the working capacity of the audit system.

8.8. The results of the security audit in the UMIS "Human Resources" (information processing operations and means of performing the audit) shall be protected against unauthorized access by applying appropriate security measures and ensuring their confidentiality and integrity.

IX. ENSURING THE INTEGRITY OF INFORMATION IN THE HUMAN RESOURCES UMIS

9.1. Ensuring the identification, logging and removal of deficiencies of software intended for information processing in UMIS "Human Resources", including the installation of patches and their renewal packages, protection against infiltration of malware in software, measures ensuring the possibility of automatic and timely renewal of means of ensuring protection against malware and virus signatures.

9.2. Illegal intrusion detection technologies and means are used, which allow monitoring of events and detection of attacks, including ensuring the identification of attempts of unauthorized use of information from UMIS "Human Resources".

9.3. Testing of the correct functioning of the security components of the UMIS Human Resources (automatically - when the system is started up, and where appropriate - at the request of the person responsible for the security policy for processing personal data).

9.4. Backups: on the basis of the volume of processing carried out, on an individual basis, the operator shall determine the time interval within which the backups of the information in the UMIS "Human Resources" and the software used for their automated processing shall be made. The backups shall be tested in order to verify the security of the information carriers and the integrity of the information indicated. Back-up restoration procedures shall be regularly updated and tested to ensure their effectiveness.

X. SECURITY INCIDENT MANAGEMENT OF SIMU HUMAN RESOURCES

10.1. The people operating the UMIS Human Resources shall, at least once a year, undergo training on their responsibilities and obligations when carrying out actions to manage and respond to security incidents.

10.2. Security incident handling includes detecting, analyzing, preventing, preventing the development, removing and restoring security. Security incidents are continuously monitored and documented in the UMIS Human Resources.

10.3. Individuals who are guilty of violating the rules on obtaining, storing, processing and protecting information from UMIS "Human Resources" shall be liable to civil, administrative and criminal liability.

XI. FINAL PROVISIONS

11.1. These Regulations are approved by the TUM Senate and revised periodically, if necessary, in case of changes in the legislation in force.
11.2. This Regulation is supplemented by the provisions of the legislation in force.
11.3. The regulation is posted on the TUM webpage, and UMIS "Human Resources" employees-operators are informed about it against signature.
11.4. Amendments and additions to this Regulation shall be made in the manner laid down for its approval.