Organization policy regarding the processing of personal data

1. General Provisions

1.1. This document (hereinafter - the "Policy") defines the policy of federal state autonomous educational institution Higher Education "St. Petersburg National Research University of Information Technologies, Mechanics and Optics "(PSRN: 1027806868154, TIN 7813045547; Address: 197101, St. Petersburg, Kronverksky pr., 49, hereinafter - the "Operator") in relation to the processing of personal data and contains, among other things, information about the requirements for the Operator to protect personal data.

1.2. The policy is approved and published on the website http://micsecs.org/ (hereinafter- the "Site") pursuant to the Terms provided for in paragraph 2 of article 18.1 Federal law of 27 July 2006 N 152-FZ "On personal data" (hereinafter - Federal law) responsibilities for the publication in a telecommunications network of the document defining the policy of the operator in relation to the processing of personal data and information about ongoing requirements for protection of personal data and to ensure access to the specified document by using the means appropriate information and telecommunications network.

1.3. The policy is developed considering the requirements of the legislation of the Russian Federations in the field of personal data. Terms Used in the Policy should be understood in the meaning defined for them in the Federal Law, if otherwise is not explicitly stated in the Policy.

1.4. The policy is available to any Internet user by clicking on the link http://micsecs.org/media/micsecs_pol_en.pdf.

1.5. The operator processes personal data of users taking into account the following principles:

- processing of personal data is carried out by the operator on a legal and fair basis;
- the processing of personal data is limited to the achievement of specific predetermined and legitimate goals. The operator has no right to process personal data incompatible with the purposes of personal data collection;
- it is not allowed to combine databases containing personal data, the processing of which is carried out for purposes incompatible with each other;
- only personal data corresponding to the purposes of their processing are subject to processing by the operator;
- the content and volume of personal data processed by the operator correspond to the stated purposes of processing. The personal data processed is not excessive in relation to their stated purposes of processing;
- when processing personal data, the reliability of personal data, their sufficiency and, if necessary, relevance in relation to the purposes of processing personal data must be ensured. The operator shall take the necessary measures to remove or clarify incomplete or inaccurate data;
- storage of personal data is in the form that allows to identify the data subject for no longer than required for the purpose of processing of personal data if the retention period of personal data not set by Federal law, the contract, which a party, beneficiary or guarantor which is the subject of personal data. Processed personal data are subject to destruction or depersonalization upon achievement of the processing purposes or in case of loss of necessity in achievement of these purposes if other is not provided by the Federal law.

2. Rights of the subject of personal data to access his personal data

2.1. The personal data subject has the right to receive the following information:

- confirmation of the fact of processing of personal data by the Operator;
- legal grounds and purposes of processing personal data;
- goals and methods used by the Operator to process personal data;
- name and location of the Operator, information about persons (for excluding Operator employees) who have access to personal data or to which personal data may be disclosed data based on an agreement with the Operator or based on the federal law;

- processed personal data relating to the relevant subject of personal data, the source of their receipt, unless a different procedure for the submission of such data is provided by Federal law;
- data retention periods for processing personal data, including periods for their storage;
- procedure for the exercise of rights by the subject of personal data, provided by Federal law
- information on completed or suspected transboundary data transfer;
- name or surname, name, patronymic and address of the person, processing personal data on behalf of Operator, if processing is entrusted or will be entrusted to such a person;
- other information required by the legislation of the Russian Federation
- Federation.

2.2. The right of the personal data subject to access his personal data may be limited in cases provided for by the legislation of the Russian Federation
Federation.

3. Operator requirements for the protection of personal data

3.1. When processing personal data, the operator shall take all necessary legal, organizational and technical measures to protect personal data from unauthorized or accidental access to them, destruction, modification, blocking, copying, provision, distribution of personal data, as well as from other illegal actions in relation to personal data.

3.2. Ensuring the security of personal data is achieved, in particular:

1) the definition of threats to the security of personal data during their processing
2) in personal data information systems;
3) the use of organizational and technical measures to ensure the security of personal data during their processing in information systems of personal data necessary to meet the requirements for
4) protection of personal data, the execution of which ensures the levels of personal data protection established by the Government of the Russian Federation;
5) by applying of the assessment procedure that has passed in accordance with the established procedure compliance with the requirements of information security;
6) by assessing the effectiveness of measures taken to ensure the security of personal data before commissioning of the information system personal data
7) taking into account machine carriers of personal data;
8) the discovery of unauthorized access to personal data and taking measures;
9) restoration of personal data modified or destroyed due to unauthorized access to them;
10) the establishment of rules for access to personal data processed in the personal data information system, as well as providing registration and accounting of all actions performed with personal data in the personal data information system;
11) monitoring of the measures taken to ensure security personal data and the level of protection of personal data information systems.