Public Institution Lithuania Business University of Applied Sciences/, 291828430

(name and code of organisation)

DESCRIPTION OF THE PROCEDURE FOR THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES, PERSONAL DATA PROCESSING/USE AND EMPLOYEE MONITORING AND CONTROL IN THE WORKPLACE

Approved by:
Public Institution Lithuania Business University of Applied Sciences
(name of issuer of the document)
~~Director Angelė Lileikienė~~
~~/signature/~~
~~6th of December, 2017 № 1.5-112~~
(date, type of the document)

L.S. /Seal: the Republic of Lithuania Klaipėda Public Institution Lithuania Business University of Applied Sciences/

SECTION I GENERAL PROVISIONS

The Description of the Procedure for the Use of Information and Communication Technologies, Personal Data Processing and Employee Monitoring and Control in the Workplace (herein further – the Procedure) of Public Institution Lithuania Business University of Applied Sciences (herein further – the College) establishes the rules for use of the College information and communication technologies, personal data management as well as the rules and extent of monitoring and control of the staff in the workplace.

SECTION II USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

1. Depending on the job performed by employees in the workplace, the College at its own discretion provides the employees with the following work equipment/facilities: a computer, mobile telephone, internet access, e-mail, access to the College internal network (Intranet), software of the College programmes (SAB, MOODLE, Cloud) and other equipment/devices of information and communication technologies.
2. Each employee of the College is given a unique name and password (-s) for login to the College network resources and/or equipment/devices of information and communication technologies. An employee shall keep the assigned password (-s) and shall not disclose it (them) to the third persons. Passwords have to be changed on a regular basis, at least once per three months, also under certain circumstances (e.g.: upon a change of an employee, a hacking threat, a suspicion that the password has become available to the third persons, etc.)
3. The provided work equipment/facilities (and tools) are the property of the College and are designated for performance of the job functions, unless otherwise individually agreed with an employee in writing upon his/her signature.
4. Notices, orders, instructions, information on salary calculated to an employee, information provided upon an employee's request, information on the changes of the rules applicable in the College as well as other information is provided to employees by e-mail – dispatching the information to their respective work e-mail addresses (the College e-mails), and if serving them via the College e-mail address is impossible – to their personal e-mail addresses; in the case of urgent necessity to perform instructions and orders – by giving the instructions over the telephone (to the College or personal telephone number).
   4.1. instructions sent by e-mail are binding for an employee and are deemed to be delivered on the next working day after their dispatch, unless the employee's confirmation of receipt of the information has been received earlier; instructions and information given over the telephone or

via a sms message are deemed to be served and binding at the moment of the call and dispatch of the sms message, respectively.

5. The employees who use e-mail, internet access and other devices of information and communication technologies provided by the College, **are strictly prohibited**:
   5.1. to publish, disseminate the confidential information of the College (including but not limited to copyright objects, internal documents of the College) on the internet, to record it to the data storage devices or to sent to a personal e-mail address or to that of the third persons, if this is not related with performance of the job functions and/or instructions of the employer.
   5.2. to use the College e-mail, internet access or equipment of information and communication technologies provided by the College for personal or commercial purposes, for activities prohibited by legislation of the Republic of Lithuania, for transmission of the information of defamatory, abusive, discriminatory, threatening character or the one contravening the principles of the public morals and order, computer viruses, unsolicited information (spam) or for other purposes that may infringe the lawful interests of the College or other persons.
   5.3. to download, install, retain, use, copy or disseminate directly unrelated to the job and/or any unauthorized, illegal, copy-right infringing or personal software/hardware and/or graphic/audio/video material.
   5.4. to send and receive data, which is (might be) virus infected, has other different programming codes, files that might impair the functioning and security of the computer or telecommunication systems, devices and software.
   5.5. to use the equipment for unlawful access to the data or systems, penetration testing and scanning of the systems, network flow monitoring.
   5.6. without permission of the College, to make unauthorised modifications and repair of hardware and software of information and communication technologies either by himself /herself or through engagement of the third persons.
   5.7. to transfer hardware and software of information and communication technologies owned by the College to the third persons if such a transfer is not related with performance of an employee's job functions or may in whichever way harm the College's interests.
   5.8. to perform other actions unrelated to performance of the job functions or contradicting the legislation.
6. When the College employees use the e-mail and internet resources for their personal purposes and/or do not comply with the requirements of the present Regulations, the College does not guarantee the confidentiality of personal information of the employees.

SECTION III PERSONAL DATA PROCESSING AND RETENTION

7. Personal data shall be processed in the College for the following purposes:
   7.1. Employees' names and surnames, personal ID number or other ID numbers, social insurance numbers, contact details (addresses of place of residence, telephone numbers and personal email addresses), details on marital status and minor children – for the purposes of concluding and performance of a labour agreement; formation of an employee's file of work records, calculation of a salary/wage and other payments due to the employees as well as their tax liabilities and tax benefits; for granting of holiday and free days for a child care (granted to mother/father), unpaid holidays, extended holidays and for other accounting purposes of the College; for provision of the details about the employees, their salaries/wages, taxes paid in respect of the employees to the governmental authorities and for other purposes related with appropriate performance of the employer's obligations.
   7.2. Details and documents on education, health condition – to the extent necessary to conclude and perform a labour agreement with employees, to ensure the appropriate labour environment for an employee and the conditions for performance of an employee's job functions.
   7.3. Employees' bank account numbers – to the extent necessary to transfer a wage/salary and other payments to the employees.
   7.4. Details on the membership in a trade union – to the extent necessary for the College to ensure the special rights of the employees related with the membership in a trade union.
   7.5. Contact details of employees – for maintaining appropriate communication when an employee is outside the workplace.

7.6. Details of customers-private persons, personal or ID codes, contact details (addresses of places of residence, phone numbers and e-mail addresses) shall be gathered, processed and used for the purposes of ordering, concluding the contracts with the customers, delivery of goods, invoicing and other purposes directly related with the service rendering to the customers as well as for the purpose of collecting the data on orders and needs of the customers.

8. The procedure for data collection and retention:
   8.1. Data about employees shall be collected with the employees' consent from the data and documents provided by the employees and/or governmental or municipal authorities.
   8.2. Data about customers shall be collected with the customers' consent by acquiring the data from the customers and gathering the data in the public domain.
   8.3. All or a part of the collected data of the employees and the customers shall be entered into the College accounting system to the extent required for the accounting purposes of the College.
   8.4. Personal data shall not be retained in the College longer than it is required for the data processing purposes and shall be destroyed when no longer needed. Every 3 years the collected and retained data shall be additionally reviewed and the unnecessary data as well as the ones, which are not subject to the legislative requirement of mandatory retention for the periods established in the legislation, shall be destroyed.
   8.5. Personal data may be archived when the legislative acts provide for the retention periods of the documents, which contain personal data, taking measures to protect the personal data and to ensure their confidentiality.
9. To attain the above purposes the College shall follow the following principles:
   9.1. necessity – the College shall collect, accumulate and use personal data only to the extent inevitably necessary for the purposes referred to herein.
   9.2. relevance – data shall be collected for a specified, clear and particular purpose, it shall be adequate in relation to such a purpose and shall not be further processed and/or retained in a manner incompliant with the purposes referred to in the present Procedure.
   9.3. transparency – data shall be collected in the College by lawful and fair methods only.
   9.4. adequacy – personal data, which is received for the purposes referred to herein, is relevant and not excessive in relation to the established purpose.
   9.5. accuracy – any data related with control of an employee is accurate and if necessary, updated on a regular basis. Inaccurate data shall be rectified or deleted.
   9.6. security – the College has implemented relevant technical and organizational measures in order to ensure security and confidentiality of any retained personal data as well as its protection from external tampering and unauthorised use.
10. Persons, whose personal data is collected, retained, stored and/or used (herein further – the Data subjects) shall have the right:
   10.1. to be informed what personal data and for what purpose are collected and processed, from what sources it has been obtained, if the sources are identifiable. Once a year the data may be provided to a person free of charge, if the scope of the requested data does not exceed the scope of a summary of the processed data. If the data is requested more often or the scope of the requested data exceeds the scope of a summary of the processed data, it shall be provided subject to payment of administrative costs for preparation and submission of such data. Amount of a fee shall be established by the director's order.
   10.2. to submit requests for rectification of inaccurate data, modification, deletion/destruction of data. Having rectified, modified, deleted the data upon a request of the Data subjects, the latter shall be informed about the rectification, modification, deletion of the data.
   10.3. by a written notice or via e-mail allowing for identification of the sender, to recall his/her consent to the collecting, retaining his/her personal data. Recall of the consent does not affect the processing of the data that has been lawfully collected prior to the recall of the consent.
11. Data protection
   11.1. Disclosure of the personal data held by the College to the third persons is prohibited, unless such a disclosure of the data is stipulated by legislative acts or orders of governmental or municipal authorities, except for the cases, when
      11.1.1. the data subject has expressed his/her consent to disclosing of such data;
      11.1.2. disclosure of the data is required for performance of agreements between the data subject and the college;

11.1.3. it is required for recovery/ enforcement of debts from the data subject;

12. or if the data transmission is urgently needed and obtaining a consent of the data subject is not possible. – sumaišyta numeracija originale

12.1. The data protection officers of the College, shall be responsible for the data processing, control, protection (by individual groups of employees). When performing his/her functions, the data protection officer of the College:

12.1.1. shall control performance of the present Procedure;

12.1.2. shall accept, analyse, perform and respond to requests of the Data subjects regarding familiarisation with the employees' data processed by the College, correction of inaccurate data, modification or destruction of such data as well as appeals against violation of the regulations of data collection and processing. Requests of the Data subjects for familiarisation with employees' data processed by the College, requests for submission of available personal data to the College, requests for rectification of incorrect data, modification or destruction of such data, as well as appeals against violation of the data collection and processing regulations shall be submitted to the Data protection officer in a written form or via e-mail, if the request submitted via email allows for identification of the data subject. Requests and appeals shall be decided no later than within 30 days as of the day of their submission and a reply to the request/appeal shall be given to the person who has submitted the request/appeal and/or to the Data subject;

12.1.3. shall implement the data protection and confidentiality measures and shall control their performance;

12.1.4. shall control and perform or charge with a task to perform a timely deletion of data when collection of the data is no longer required for the purposes provided in the Procedure or the Data subject recalls his/her consent to the data processing. Also, shall control that copies of documents containing personal data are destroyed in such a manner that to make authentication of such documents and retrieval of their contents impossible;

12.1.5. shall notify the Data subject on breach of the data security if the breach may pose a threat to the rights of the Data subject;

12.1.6. shall perform other functions provided by the present Procedure in order to ensure implementation of the provisions of the Procedure, its purposes and principles.

12.2. The data protection officer of the College (authorised person) and all employees of the College appointed by an order of the director to process personal data or processing personal data as a result of their job functions shall observe the principle of confidentiality and shall keep any information related with the personal data, an access to which they have acquired in the course of performance of their job functions, as confidential, unless such information is in the public domain pursuant to the provisions of current legislation or other legislative acts. The obligation to maintain confidentiality of personal data shall survive the transfer to other job and the expiry/termination on whatever grounds of the labour or contractual relationships.

12.3. The data protection officer of the College (authorised person) and all employees of the College working with the employees' data shall take measures to prevent an accidental or unlawful destruction, tampering, disclosure of the personal data, as well as any other unlawful processing or use, by keeping the documents and document files in a safe and appropriate manner and by avoiding making unnecessary copies. If an employee has doubts regarding reliability of the implemented security measures, he/she shall contact the data protection officer of the College, and the latter – the Head of the College in order to make an assessment of available security measures and, if necessary, to initiate acquisition and implementation of additional measures.

12.4. A person responsible for computer maintenance (IT administration) must ensure that personal data files are not shared on other computers, and anti-virus software is updated at least once per week.

12.5. At least once per month a person responsible for the computer maintenance (IT administration) shall make copies of the data files contained in the computers.

SECTION IV MONITORING AND CONTROL OF THE WORK EQUIPMENT/FACILITIES AND THE WORKPLACE

13. The College shall organize and carry out monitoring of the processes of use of the provided work equipment/facilities and exchange of professional (and in certain cases – personal or other) information carried out through electronic means of communication or otherwise.
14. When organizing the monitoring, the College shall apply the monitoring measures adequate to the intended purposes and only in the cases when it is impossible to attain the control and monitoring purposes by means that are less invasive to the employees' privacy.
15. The purposes of monitoring and control in the workplace:
    15.1. to protect confidential information of the College from its disclosure to the third persons.
    15.2. to protect personal data of the College customers and employees from unlawful transmission to the third persons.
    15.3. to protect the College information systems from hacking, data thefts, viruses, harmful websites, malicious software, infringement of copyrights through the College equipment and the internet access.
    15.4. to protect the College property and to ensure security of people within the College premises or territory.
    15.5. to protect the proprietary interests of the College and to ensure performance of the work duties.
16. To attain the above mentioned purposes, the College shall follow the following principles:
    16.1. necessity – prior to applying the forms of employee control as described herein, the College shall make sure that the intended form of control is inevitably necessary for attainment of the established purposes.
    16.2. relevance – data is collected for an established, clear and particular purpose and shall not be further processed and/or retained in a manner that is in conflict with the purposes specified in the present Procedure.
    16.3. transparency – any secret video, e-mail, internet surveillance or monitoring of the software use in the College is prohibited except for the cases when such a surveillance is permitted by laws or when pursuant to the laws such actions of the College are permitted in order to detect violations in the workplace.
    16.4. adequacy – personal data, which is obtained through the process of control referred thereto, is relevant and not excessive in relation to the established purpose.
    16.5. accuracy and data retention – any data related with the employee control is accurate, is subject to regular updating, if necessary, and shall be lawfully retained for no longer than it is necessary.
    16.6. security – the College has implemented respective technical and organisational measures in order to ensure that any retained personal data is secure and protected from external tampering.
17. For the purposes referred to in the Procedure and following the principles laid out in the Procedure, the following measures are implemented in the College:
    17.1. use of software to track location of the vehicles owned and used by the College;
    17.2. use of software to automatically keep records of the employees' internet browsing history, which shall be retained for 6 months/years. The retained data of the employees' browsing history shall not be subject to continuous monitoring, they shall be reviewed only in the event of a reasonable suspicion of violation of laws or an employee's duties and only to the extent related to eventual violation.
    17.3. the College may check the contents of the communication programmes (e.g.: Skype, Viber, Messenger, Facebook, Instagram, etc.) in the computers and telephones assigned to employees, other e-communication and internet browsing history to the extent required for effectuation of the purposes provided in the present Procedure and to the extent necessary to ensure that the work equipment/facilities of the College are not used for the purposes and for the performance of the tasks unrelated with the job functions of an employee.
    17.4. the College, without a separate warning, may restrict access to particular websites, communication programmes or software. If the above measures are insufficient, the College may for the purposes specified herein check how an employee complies with the requirements on use of the College e-mail and internet resources, when investigating incidents/violations, as well as may submit the equipment used by the employees to the third persons for the purpose of investigation.
    17.5. the College, having put a visual warning sign, may install video surveillance devices within the College premises and/or territory.

17.6. If the need arises, the College, subject to a prior notification to employees, may apply other means of the employee surveillance and control (e.g. sound recording, etc.).

18. Hereby the employees are informed about the rights of the College and its eventual actions to ensure attainment of the purposes provided in the Procedure.

SECTION V FINAL PROVISIONS

19. The present Procedure shall be revised and updated when required or upon changes in the legislation that regulates the legal relationships in this field.
20. The present Procedure shall be binding to all employees of the College. The employees shall be made aware of the present Procedure and its amendments upon personal signature or through electronic means of communication and shall undertake to comply with its provisions. Violations of the present Procedure may be considered to be violations of an employee's job duties and may result in liability provided in the Labour Code of the Republic of Lithuania.
21. Familiarisation of the employees with the Procedure, its amendments as well as their consent to the processing of their personal data and to surveillance of their work equipment/facilities and the workplace shall be expressed in writing by undersigning a consent or through electronic means of communication that allow identification of the undersigned person.
22. The Council of Employees of the College has been informed about the present Procedure and their consultation regarding the present Procedure has been obtained.

The undersigned hereby confirm by their respective signatures that:

1. they have read the above referred procedures, have familiarised with them, have understood the Procedure for Use of Information and Communication Technologies, Personal Data Processing and Employee Monitoring and Control in the Workplace and undertake to comply with its provisions.
2. they freely give their consent to their personal data processing in the College pursuant to the procedure and for the purposes established herein.
3. they freely give their consent to video surveillance and recording pursuant to the procedure and for the purposes established herein.