INFORMATION TECHNOLOGY SERVICE CENTER
OF VILNIUS UNIVERSITY

O R D E R

ON THE APPROVAL OF THE DESCRIPTION OF THE PROCEDURE FOR THE INVESTIGATION OF CRITICAL INCIDENTS IN RELATION TO ELECTRONIC INFORMATION SECURITY OF SYSTEMS MANAGED BY THE ITPC

18 December 2018

No. (1.1) 640000-DV-16

1. I hereby a p p r o v e the Description of the Procedure for the Investigation of Critical Incidents in Relation to Electronic Information Security of Systems Managed by the VU ITPC.
2. To declare the ITTC Director's Order No. 520000-DI-16 -(5201.DĮ) of 14 July 2015 void.

Director of the Information Technology Service Center Arūnas Stašionis

APPROVED
by Order No. 640000-DV-16
of 18 December 2018 of the Director of the ITPC

DESCRIPTION OF THE PROCEDURE FOR THE INVESTIGATION OF CRITICAL INCIDENTS OF ELECTRONIC INFORMATION, CYBERSECURITY, AND PERSONAL DATA SECURITY WITHIN INFORMATION SYSTEMS MANAGED BY THE ITPC OF VILNIUS UNIVERSITY

I. GENERAL PROVISIONS

1. The Description of the Procedure for the Investigation of Critical Security Incidents of Electronic Information, Cybersecurity, and Personal Data within Information Systems Managed by the ITPC of Vilnius University (hereinafter the 'IS') and IT Services (hereinafter the 'critical incidents' and the 'Description', respectively) establishes the actions of the information systems maintained by the VU ITPC (unless otherwise specified in the electronic information security documents of the said systems), as well as the actions of the users, administrators, security representatives, and the members of the investigation group for security incidents of information systems (hereinafter the 'Group'), and the actions regarding computer networks when investigating disruptions in the functioning, data processing, and provision of hardware and software of information systems that occur during critical incidents, when they are identified based on the criteria established in the Activity Continuity Plan.

2. Terms defined in the Description:

2.1. Escalation – reclassification of incident categories and/or involvement of unit managers and/or services with greater authority in incident resolution.

2.2. Information system – the entirety of information technology resources and software managed by the VU ITPC to provide information and technical support for one or more activity processes.

2.3. Information technology services (hereinafter the 'IT Services') – information and data transmission services provided by the ITPC to the University community, Lithuanian educational and research institutions, as well as other institutions in Lithuania or abroad.

2.4. System administrator – the employee responsible for the use of the infrastructure resources allocated to the information system and for ensuring their operation and the security of electronic information by technical means.

2.5. Critical incident – an event or activity in cyberspace that enables or may enable or allow unauthorised access to, disruption of or modification of, including takeover of, an information system, an electronic communications network or an industrial process

control system, or destruction or damage to an information system, an electronic communications network or an industrial process control system, erasure or alteration of electronic information, including but not limited to personal data, withdrawal or restriction of access to electronic information, or enabling the misappropriation or other use of non-public electronic information by persons not authorised to do so, and the consequences of the incident meet the criteria for assessing the criticality of the incident as set out in the ITPC Activity Continuity Management Plan.

2.6. Other terms used in this Description are defined in the legal acts referred to in Item 3 of the Description.

3. Critical incidents shall be managed in accordance with:

3.1. the Republic of Lithuania Law on Electronic Communications;

3.2. the Republic of Lithuania Law on Legal Protection of Personal Data;

3.3. the Republic of Lithuania Law on Legal Protection of Personal Data, Processed for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences, the Execution of Criminal Penalties, or National Safety or Defence;

3.4. Resolution of the Government of the Republic of Lithuania No. 716 of 24 July 2013 "On Approval of the Description of General Electronic Information Security Requirements, Description of Content of Safety Documentation Guidelines and Description of Classification of State Information Systems, Registers and Other Information Systems and Determination of the Importance of Electronic Information Guidelines";

3.5. Order of the Director of the State Data Protection Inspectorate No. 1T-53(1.12.) of 24 May 2018 "On Approval of the Recommended Form of Notification about Personal Data Security Breach";

3.6. Order of the Minister of National Defence No. V-11 of 6 January 2019 "On the Description of the Procedure for National Cyber Security Centre Reaction to Cyber Incidents in the State's Information Resources and Critical Information Infrastructure";

3.7. Order of the Vilnius University Chancellor No. R-265 of 20 June 2017 (wording of Order of Vilnius University Chancellor No. R-145 of 14 March 2018) "On Amendments of the ITPC Regulations and Approval of the ITPC Unit Regulations";

3.8. the Rules of Processing of Personal Data of Studying Persons in Vilnius University, approved by Resolution of the Commission of Vilnius University Senate No. SK-2013-8-7 of 20 June 2013;

3.9. the Description of the Procedure for Personal Data Processing at Vilnius University, approved by Order of the Rector of Vilnius University No. R-316 of 25 May 2018 "On Approval of the Description of the Procedure for Personal Data Processing at Vilnius University";

3.10. the Rules for the Processing of Personal Data for the Purposes of Scientific Research in Vilnius University, approved by Order of the Rector of Vilnius University No. R-452 of 23 November 2015 "On Approval of the Rules for the Processing of Personal Data for the Purposes of Scientific Research in Vilnius University";

3.11. the Vilnius University Rules of Procedure, approved by Order of the Rector of Vilnius University No. R-146 of 20 April 2015;

3.12. the Study Regulations of Vilnius University, approved by Resolution of the Senate of Vilnius University No. SK-2012-12-8 of 21 June 2012;

3.13. the Vilnius University ITPC Activity Continuity Management Plan, approved 14 March 2015 by Order of the Rector of Vilnius University No. R-83;

3.14. Order of the VU Chancellor No. R-335 "On IT Hardware Hosting in the VU Data Centre", approved 9 September 2016;

3.15. the Description of Services of IT Hardware Hosting in the Vilnius University ITPC Data Centre, approved by Order of the Director of the VU ITPC of 3 December 2018 (1.1) 640000-DV-14.

II. RECORDING OF SAFETY INCIDENT REPORTS AND IMMEDIATE ACTION TO STOP THE DEVELOPMENT OF SAFETY INCIDENTS

4. An ITPC employee or any user, suspecting a safety incident or indications of it, shall immediately report it to IT Helpdesk at pagalba@itpc.vu.lt and/or by telephone at 8 (5) 236 6200 (during office hours from 8:00 to 17:00).

5. The safety incident report shall be recorded in the IT Help system at https://veiklos.vu.lt/projects/ITPC/issues and assigned to:

5.1. the system administrator – to resolve the incident;

5.2. the head of the responsible unit – to monitor the incident and/or, in the cases specified below, investigate it;

5.3. the authorised person of the data security of the related information system – to monitor the incident and/or, in the cases specified below, investigate;

5.4. the Information Security Officer – to monitor the incident and/or, in the cases specified below, investigate it.

6. The IT Helpdesk employee, after assessing the criticality of the incident and the progress of its resolution, shall have the right to escalate the resolution of the incident to the head of the unit responsible for the service provision;

7. The head of the unit responsible for handling the incident shall assess within four working hours whether the incident can be resolved within the timeframe set out in Annex 6 of the activity continuity plan for the category of incident, and shall escalate the incident by convening an Activity Recovery Team meeting provided for that the expected timeframe for resolution of the incident is likely to exceed the criteria set in the Activity Continuity Plan.

8. If the incident is resolved within the minimum timeframes set out in the activity continuity plan for the resolution of the incident, the head of the responsible unit shall assess the progress of the resolution in the JIRA information system and make a decision to close the incident.

9. Incidents whose consequences and handling circumstances meet the criteria for critical incidents shall be investigated in accordance with the following procedure.

10. If the head of unit assesses that the incident may have a greater impact if the incident cannot be resolved within 24 hours, the incident shall be escalated by further informing the head of the activity recovery management team (Director of the ITPC or the Acting Deputy) of the situation.

11. The Information System Data Security authorised person, or, if no such person has been appointed, the Information Security Officer shall, upon receiving a notification of a critical security incident and after assessing the circumstances of the incident, reclassify the security incident, organise the gathering of the necessary material for the investigation, inform other related employees and, if necessary, the relevant authorities.

12. In the event of an incident, the system administrator shall inform the immediate superior or, in their absence, the Helpdesk, with a request to inform the immediate superior, and shall immediately take all reasonable precautions and, without causing damage to the services and systems provided:

12.1. take immediate administrative action to stop the spread of the security incident;

12.2. activate the save mode of the administrative actions or, if this is not available, copy the administrative commands to a text medium, recording the timestamps of the actions;

12.3. save existing copies of the data, system records and configuration of the equipment at the time of the incident for the purposes of the investigation;

12.4. inform their immediate superior upon assessment that the incident may be classified as critical in accordance with the criteria described in Annex 6 of the ITPC Activity Continuity Management Plan;

12.5. after localising the incident and stopping its spread, make available to the IT Helpdesk the system records relevant to the category of the system, necessary for the investigation of the incident. This shall include recorded network events, the actions taken to copy personal data, if any, and to restore it in the event of its accidental loss (when and by whom the said actions were taken), and information on data recorded in the information system, the activation and deactivation of the information system, the success and failure of attempts to register with the information system, any actions taken by users of the information system, and any other security-relevant events (information provided by Item 7.7 of Order of the Minister of the Interior No.1V-832 of 4 October 2013), the information specified in Annex 1 to the Republic of Lithuania Law on Electronic Communications, and, if possible, other information necessary for the investigation.

13. Upon suspicion of an unlawful act that violates or will imminently violate the security of an information system, the ITPC Information Security Officer shall inform the Director of the ITPC, the representative(s) of the controller(s) of the information system(s), and, if necessary, the competent authorities investigating incidents of electronic communication networks, protection of personal data, information security incidents, unlawful acts related to electronic information security incidents, in the established procedure.

14. Upon assessment that a critical incident has occurred, the immediate superior of the administrator shall inform the head of the activity continuity plan management team, who shall make a decision on the remediation of the activity incident and the activity recovery actions.

III. INVESTIGATION OF SAFETY INCIDENTS

15. In the event of a non-critical incident, the investigation of the safety incident shall be conducted by the responsible head of the division.

16. By the order of the responsible head of the division, the materials for the investigation shall be collected and provided by the administrators of associated systems.

17. In the event of a critical incident, the resolution of the safety incident shall be organized by the responsible head of division, investigation of the incident is organized by the system data security authorised person, and if the incident is not removed within one working day, the investigation of the incident is transferred to the ITPC Information Security Officer.

18. The administrator must disclose the progress of the investigation by submitting the information to the registered incident description in the incident log at https://veiklos.vu.lt/projects/ITPC/issues no later than at the end of the working day.

19. If investigation tasks need to be assigned to employees of other VU units, the head of the responsible division shall address the head of the required unit.

20. After the employees have completed the assigned tasks, the head of the responsible division shall fill out the incident investigation report and forward the information to the ITPC Information Security Officer.

21. The conclusions of the non-critical incident investigation shall be confirmed in the safety incident log and the investigation shall be closed by the head of the responsible division.

22. Upon determining that the incident is critical, the ITPC Information Security Officer may form a security incident investigation group (hereinafter the 'Group').

23. Investigations of critical incidents shall be carried out in the Group according to the procedure set out in Items 24-31.

24. In the event of a critical incident, no later than the next working day after the registration of the safety incident, the head of the unit handling the incident shall call a Group meeting.

25. The composition of the Group is approved by an order of the Director of the ITPC and updated when necessary.

26. The ITPC Information Security Officer shall lead the Group and inform the Director of the ITPC and related authorised persons of the IS data management about the process of investigations.

27. To determine the circumstances of the security incident, the reasons and the persons who may have caused the security incident due to illegal actions, the ITPC Information Security Officer shall assign the security incident investigation tasks to the members of the Group.

28. Group members have the right to:

28.1. inspect the safety incident site and equipment;

28.2. review system records related to the incident;

28.3. interview users potentially involved in a security incident;

28.4. get acquainted with the documents necessary for the investigation of the safety incident;

28.5. receive other information related to the security incident;

28.6. propose administrative and technical electronic information security measures;

28.7. participate in restoring of the activities of the IS activity continuity.

29. Group members must:

29.1. based on the collected research material, write the conclusion of the safety incident investigation, in which the circumstances, reasons and supporting evidence of the safety incident are set out, and as the persons whose activities may have caused the safety incident are indicated as well;

29.2. draw up risk reduction action plans within the limits of their competence;

29.3. cooperate with telecommunication network cyber security response groups (CERT, CSIRT);

29.4. cooperate with special services for liquidating damage and competent authorities for investigating electronic communication networks, information security incidents, illegal acts related to electronic information security incidents;

29.5. by instruction of the Head of the ITPC, prepare drafts of the detailed plan for the restoration of IS activities or the projects of reforms or additions to the documents implementing IS security.

30. After receiving the critical incident investigation material specified in Item 12.5 of the Description, the ITPC Information Security Officer shall submit concluding remarks in the JIRA system, fill in the critical incident registration log (Annex 2 to the ITPC Activity Continuity Management Plan).

31. After the Group has completed the assigned tasks, the ITPC Information Security Officer shall register the critical incident investigation report in the document management system AVILYS and inform the Director of the ITPC and the participants of the investigation.

IV. FINAL PROVISIONS

32. If the employees or students are identified for causing an incident due to their inappropriate actions or inactions, such persons must provide an explanation, addressed to the VU ITPC, of the circumstances that influenced the incident.

33. Violations potentially committed by employees shall be examined according to the procedure established by Order of the Chancellor of Vilnius University No. 447 of 13 October 2017 “On the Approval of the Description of the Procedure for Examining Violations of the Work Duties of Vilnius University Employees”.

34. Violations that may be committed by students shall be dealt with in the Study Regulations of Vilnius University, approved by Resolution of the Commission of Vilnius University Senate No. SK-2012-12-8 of 21 June 2012 (wording of Resolution of Vilnius University Senate No. S-2018-5-2 of 22 May 2018) and the procedure established in related legal acts.

35. Violations potentially committed by employees shall be reported to their immediate superiors; violations committed by students and listeners shall be reported to the heads of the respective core departments; violations potentially committed by other persons with contractual relationships shall be reported to the heads of university units that have concluded these contracts.

36. In case that liability is provided for in the legal acts of the Republic of Lithuania, violations potentially committed by individuals shall be reported to the competent institutions.

37. The decisions by the employees solving the incident, the managers conducting the investigation, and the Director of the ITPC, made according to this Description, are considered to have been made since the publication and must be documented in the IT Support system.

38. Safety incident investigation materials shall be stored for at least one year for non-critical incidents and three years for critical incidents from the date of registration of the safety incident.

_____