DATA BREACH PROCEDURE

Owner: **Data Protection Officer**

Approved by: **Director of Administration and Finance**

Campus Director

Update History: May 2020

June 2020

Neapolis University Pafos

Table of Contents

1. Scope

This procedure applies University-wide and to all University information, regardless of format.

It applies to all staff, students, contractors and visitors to the University.

The responsibilities of data processors acting on the University's behalf in respect of data incidents are set out in the relevant agreement.

2. Responsibilities

2.1 Information Users

It is the responsibility of all information users to report genuine, potential, suspected and threatened Data Protection Incidents and to assist with investigations as required, especially if urgent action must be taken to avoid additional damage.

2.2 Heads of Departments and Directors

Heads of Departments and Directors are required to ensure that their staff follow this procedure and that they assist with any ensuing investigation.

2.3 Incident Management Staff

University staff with specific responsibilities for receiving data protection incident reports and for initiating investigations are:

α. Data Protection Officer (DPO)

β. Chief Information Officer (CIO)

γ. Campus Director

Incident reports may be received and escalated by IT Support, IT Management and staff.

2.4 Data Protection Officer (DPO)

The Data Protection Officer is solely responsible for deciding whether a report should be made to the Office of the Commissioner for Personal Data Protection, whether other parties should be informed and for communication of the relevant information as required.

The DPO will maintain a record of all data incidents involving personal data irrespective of whether or not the incident is reported to the Office of the Commissioner for Personal Data Protection as a data breach.

3. Breach Management/ Reporting to the Office of the Commissioner for Personal Data Protection

3.1 Data Protection Incidents must be reported immediately and notified by following the reporting guidance set out in this procedure:

● Incidents must be reported either via telephone or leaving a voicemail to the Data Protection Office tel no. +357 26843346 or via email to dpo.nup@nup.ac.cy

The DPO will monitor this account and arrange for appropriate action to be taken once a report has been received.

● The report should include full and accurate details of the incident including who is reporting it and what kind of data is involved. As part of the reporting process, the "Data Protection Incident Report" form should be completed (see:

http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2g_gr/page2g_gr?opendocument).

● Once a data protection incident has been reported, an initial assessment will be made by the DPO and/or the CIO and/or the Campus Director and/or the relevant staff of the University to establish the veracity of the report and severity of the incident. This will then inform the decision about who the responsible lead investigator officer should be (see Appendix A).

● According to the collection of the findings the DPO and/or the CIO and/or the Campus Director and/or the relevant staff of the University will assess whether the incident poses a risk to the rights and freedoms of individuals and whether the Office of the Commissioner for Personal Data is required to be informed. According to the article 33, the Controller will have to report the violation, unless the infringement is unlikely to endanger the rights and freedoms of individuals.

● The Controller notifies the Office of the Commissioner for Personal Data immediately within 72 hours of being informed of the fact of the personal data breach, unless it has been assessed that the incident does not endanger the rights and freedoms of individuals. The Controller is responsible for providing at least the following information to the Commissioner:

▪ Description of the nature of the violation and possible consequences of the incident.

▪ Categories and approximate number of data subjects affected by the incident.

▪ Categories of personal data and number of affected files containing personal data.

▪ Possible consequences of the violation.

▪ Measures that have been taken or have been immediately proposed to be implemented in order to address the incident of violation and / or to limit its effects.

▪ Name and contact details of the DPO and / or another person who may provide information.

If the notification to the supervisory authority does is not made within 72 hours, it shall be accompanied by reasons for the delay according to article 33 par. 1 GDPR.

3.2 If the Data Protection Incident has any IT security elements - for example, a user account was compromised as part of a phishing campaign - the University's Service Desk must also be alerted, clearly stating that this is related to a data protection incident.

3.3 Breach management has four critical elements

● Containment and recovery

The goal is to limit any damage as far as possible

● Assess the ongoing risks

The assessment will help to guide decisions on which remedial actions have to be taken as well as whether and who will have to be notified.

● Notifying the appropriate people/organizations

This would only be done after an assessment has taken place and only by appointed staff**.**

● Evaluation

Both of the incident at hand, how it was handled and whether steps can be taken to avoid a future occurrence of the same type of incident.

The activities and points for consideration will be mentioned in the 'Incident Checklist'. The responsible investigator should also complete an 'Activity Log' recording the timeline of the incident management.

3.4 Heads of Departments and Directors will work with relevant stakeholders, the DPO, the CIO and the Campus Director and their nominees to investigate and resolve any reported incidents in their area of responsibility.

3.5 If a third party organization's data is affected, the department holding said data has to alert and consult the Data Protection Officer immediately.

4. Incident Review

4.1 The DPO office will review incidents regularly, including whether the procedure was adhered to, to address possible reoccurrences of incidents and to address any new risks that were highlighted as part of the investigation.

4.2 The reviewing process will allow identifying necessary adjustments to the Data Breach Procedure, to existing policies or the need for new policies.

5. Appendix

Appendix A- Data Classification

All reported incidents have to include the relevant data classification so that the associated risks can be accurately assessed:

- **Public Data**

Information which is either intended for public use or which could be made public without any adverse impact on the University.

- **Internal Data**

Information which is related to the day-to-day activities of the University. It is mainly intended for use by staff and students, although some data might be helpful to third parties working with the University.

- **Confidential Data**

Information which is related to the more sensitive nature of procedures and processes of the University which represent the essential intellectual capital and knowledge. Access to this kind of information should only be granted to those people who need to know it in order to fulfil their role within the University.

- **Highly Confidential Data or Personal Data**

Information that, would cause significant damage to the University's business activities or reputation, if it should be released. Access to this kind of information should be highly restricted to staff which has the need and right to access and/or modify this specific set of data.

……