UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Internal university reporting of an information security incident

(As of 01.10.2018)

This form must be used to report incidents that affect or could potentially affect information security, i.e. the security of processing operations or the protection of personal data, immediately after the incident is known. This applies to reporting all attacks on IT systems, security incidents or suspected unauthorized handling of sensitive and/or personal data (information security incidents).

Fill in the fields (text boxes) with as much information/facts as is currently available. To assist, there are completion instructions at the end of this document. If available, consult management and/or the data protection coordinator for the respective department and, if necessary, colleagues or administrators. E-mail the completed report form to the following address:

vorfall@upb.de.

The incident report will be processes and evaluated by an "incident team". If necessary, the incident team, in consultation with the executive committee must report the incident to the supervisory authority or inform all persons concerned. Inquiries may arise regarding the necessary evaluation, and due to these inquiries, it is essential to provide contact information. If necessary, measures are to be taken and coordinated as quickly as possible in order to limit the consequences of the incident. In any case, the processor will receive final feedback on the reported incident.

(Background: A data security or data protection incident can result in violations/breaches of the protection of personal data, which, in accordance with Art. 33 of the EU General Data Protection Regulation, must be reported to the supervisory authority within 72 hours of becoming known if the violation/breach poses risks for the data subjects or if risks may arise.)

Designation / Name		
Responsible area / Department		
Processor / Person reporting		
Contact Info. (Phone, E-mail)		
If applicable, additional contact persons		
Contact Info. (Phone, E-mail)		
Date, time of incident (if known)		
Date, time of knowledge (becoming aware) of the incident		
Affected system / database, etc.		

Description of the incident	
Is personal data affected?	☐ Yes, ☐ No, ☐ Unsure
Number of potential persons affected	
Type(s) of potential data affected (e.g., names, addresses, e-mail addresses, examination lists, list of participants of…, certificates, applications, unpublished research results, patent data, etc.)	
Consequences regarding the data	☐ Destruction / Loss, ☐ Modification, ☐ Unauthorized disclosure
Impact on persons / or to the university	
Cause (probable cause)	
Immediate actions already implemented	
Further planned / possible actions to consider	

Completion instructions / Assistance

Designation / Name: meaningful designation of the incident (e.g. successful hacker attack on personnel database, theft of a workstation computer, USB stick lost on the train)

Responsible area / department: description of the area in which the incident took place, which is as differentiated as possible (name of the department, subject area, faculty, institute, working group, facility, etc.)

Processor / person reporting: name and position (e.g. system administrator, clerk)

Contact Info: (phone, e-mail): for inquiries

If applicable, additional contact persons: name and position (e.g. department manager)

Contact Info: (phone, e-mail): for inquiries

Date, time of incident: if known, when did the incident happen?

Date, time of knowledge of the incident: when did the person reporting/the university become aware of the incident?

Affected system / database, etc.: if possible, which IT infrastructure, hardware and/or software is affected by the incident; if available server name(s)

Description (Name) of the incident: What exactly happened? Description of the type of event that is as meaningful as possible (e.g. when administering authorizations in the campus management system, there was an error in the assignment of groups and authorizations. As a result, all lecturers of the Faculty of Medicine (group "Medical Lecturers") from 01.06.2018 to 31.7.2018 (noticing the incorrect configuration) to access the course of studies and examination data of all students at the university. ...)

Is personal data affected? If known, indicate whether personal data was affected by the incident. (Personal data is information that makes it possible to identify a person. In addition to direct personal information, such as name, date of birth, telephone number or IP address, this is also data about personal characteristics, beliefs or relationships, which may allow conclusions regarding a specific person.)

Number of potential people affected: rough estimate of how many people are affected or, if not exactly known, the potentially number that may be affected (e.g. all students (20,000), approx. 300 participants in the survey)

Type(s) of potential data affected: e.g. names, addresses, examination data, personal data, registration for events, bank details (account data), health data, etc.

Consequences regarding the data: What happened to the data or could possible happen? Data destroyed or deleted, data was changed/modified, data disclosed without authorization / unlawfully published, etc.

Impact on persons / or to the university: What effects/impact does the incident have or could the incident have? (For example, examination data from the area ... came to the attention of the following unauthorized groups of people ... within the university; publication of patent data, which jeopardizes a planned patent application by the university)

Cause / (probable) cause: What caused the error? (For example, human error due to imprecise work (input errors), technical problem in the application, misconfiguration / security gap due to missing updates that were exploited by a hacker.)

Immediate actions already implemented: Description of the immediate measures/actions taken to limit the consequences of the incident (e.g. shutdown or disconnection of the affected server, blocking of users who are affected by incorrectly assigned authorizations)

Further planned / possible actions to consider: What other actions must/should be implemented so that the impact on the people affected remains as low as possible and safe normal operations may be restored? (E.g. correction of the program error and extensive tests; importing the currently published security patches ..., letter to the persons who were able to gain access to data without authorization, with the request to delete this data and to treat the content confidentially, future use of a secure encryption method, etc.)