UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Hochschulinterne Meldung eines Informationssicherheitsvorfalls

(Stand 1.10.2018)

Mit diesem Formular müssen Vorfälle, die die Informationssicherheit, d. h. die Sicherheit von Verarbeitungen oder den Schutz personenbezogener Daten beeinträchtigen oder auch bereits beeinträchtigen könnten, möglichst unmittelbar nachdem sie bemerkt wurden, gemeldet werden. Das betrifft sämtliche Angriffe auf die IT-Systeme, Sicherheitsvorfälle oder Verdachte auf den unerlaubten Umgang mit sensiblen und/oder personenbezogenen Daten (Informationssicherheitsvorfälle).

Füllen Sie die Felder soweit möglich und Ihnen die Fakten bereits bekannt sind aus. Am Ende des Dokuments finden Sie Ausfüllhinweise. Ziehen Sie soweit zeitnah verfügbar die Leitung und/oder die Datenschutzkoordinatorin / den Datenschutzkoordinator Ihres Bereichs und wenn erforderlich Kolleginnen, Kollegen, Administratorinnen oder Administratoren hinzu. Senden Sie das ausgefüllte Meldeformular per E-Mail an die Adresse

vorfall@upb.de.

Der Vorfall wird von einem „Vorfallteam“ bearbeitet und bewertet. Ggf. muss durch das Vorfallteam in Rücksprache mit dem Präsidium eine Meldung an die Aufsichtsbehörde erfolgen oder es sind die betroffenen Personen zu informieren. Für die dazu erforderliche Bewertung können Rückfragen erfolgen, weshalb unbedingt ein Kontakt anzugeben ist. Ggf. sind möglichst schnell Maßnahmen zu ergreifen und abzustimmen, um die Folgen des Vorfalls zu beschränken. Sie erhalten in jedem Fall eine abschließende Rückmeldung zum gemeldeten Vorfall.

(Hintergrund: Aus einem Datensicherheits- oder Datenschutzvorfall können sich Verletzungen des Schutzes personenbezogener Daten ergeben, die gemäß Art. 33 der EU-Datenschutz-Grundverordnung binnen 72 Stunden nach Bekanntwerden an die Aufsichtsbehörde gemeldet werden müssen, wenn aus der Verletzung Risiken für die betroffenen Personen entstehen können.)

Bezeichnung / Benennung		
Verantwortlicher Bereich		
Bearbeiter / meldende Person		
Kontakt (Tel., E-Mail)		
Ggf. abweichende Ansprechperson		
Kontakt (Tel., E-Mail)		
Datum, Uhrzeit des Vorfalls (sofern bekannt)		

Datum, Uhrzeit der Kenntnis des Vorfalls	
betroffenes System / Datenbank etc.	
Beschreibung des Vorfalls	
Sind personenbezogene Daten betroffen?	☐ ja, ☐ nein, ☐ unklar

Anzahl (möglicherweise) betroffener Personen	
Art der (möglicherweise) betroffenen Daten (bspw. Adressen, E-Mail-Adressen, Prüfungslisten, Teilnehmerlisten von …, Zeugnisse, Bewerbungen, unveröffentlichte Forschungsergebnisse, Patentdaten)	
Konsequenzen bzgl. der Daten	☐ Vernichtung / Verlust, ☐ Änderung, ☐ unbefugte Offenlegung
Auswirkungen auf Personen / auf die Universität	.
(Wahrscheinliche) Ursache	
Bereits ergriffene Sofortmaßnahmen	
Weitere geplante / mögliche Maßnahmen	

Ausfüllhinweise / Hilfe

Bezeichnung / Benennung: aussagekräftige Bezeichnung des Vorfalls (bspw. erfolgreicher Hackerangriff auf Personaldatenbank, Diebstahl eines Arbeitsplatzrechners, in der Bahn verlorener USB-Stick)

Verantwortlicher Bereich: möglichst differenzierte Bezeichnung des Bereichs in dem der Vorfall stattfand (Name des Dezernat, des Sachgebiets, der Fakultät, des Instituts, der Arbeitsgruppe, der Einrichtung, …)

Bearbeiter / meldende Person: Name und Rolle (bspw. Administrator des Systems, Sachbearbeiter)

Kontakt (Tel., E-Mail): für Rückfragen

Ggf. abweichende Ansprechperson: Name und Rolle (bspw. Leiter des verantwortlichen Bereichs)

Kontakt (Tel., E-Mail): für Rückfragen

Datum, Uhrzeit des Vorfalls: sofern bekannt, wann fand der Vorfall statt

Datum, Uhrzeit der Kenntnis des Vorfalls: wann erlangte die meldenden Person / die Universität Kenntnis vom Vorfall

betroffenes System / Datenbank etc.: sofern möglich, welche IT-Infrastruktur, Hard- und/oder Software ist vom Vorfall betroffen ist; ggf. Servername(n)

Beschreibung des Vorfalls: Was ist genau passiert? Möglichst aussagekräftige Beschreibung über die Art des Ereignisses (z. B. Bei der Administration von Berechtigungen im Campusmanagementsystem erfolgte ein Fehler bei der Zuordnung von Gruppen und Berechtigungen. Dadurch konnten sämtliche Dozenten der Fakultät Medizin (Gruppe „Medizindozenten“) vom 1.6.2018 bis zum 31.7.2018 (Bemerken der Fehlkonfiguration) auf die Studienverläufe und Prüfungsdaten sämtlicher Studierenden der Universität zugreifen. …)

Sind personenbezogene Daten betroffen?: Geben Sie sofern bekannt an, ob von dem Vorfall personenbezogene Daten betroffen sind.
(Personenbezogene Daten sind Informationen, die eine Identifizierung einer Person möglich machen. Neben direkten Angaben zur Person, wie Name, Geburtsdatum oder Telefonnummer oder IP-Adresse, sind dies auch Daten über persönliche Merkmale, Überzeugungen oder Beziehungen, die den Rückschluss auf eine bestimmte Person ermöglichen.)

Anzahl (möglicherweise) betroffener Personen: grobe Einschätzung wie viele Personen betroffen sind oder sofern nicht genau bekannt ggf. betroffen sein könnten (bspw. alle Studierenden (20.000), ca. 300 Teilnehmer der Befragung)

Art der (möglicherweise) betroffenen Daten: bspw. Namen, Adressen, Prüfungsdaten, Personaldaten, Anmeldungen zu Veranstaltungen, Bankverbindungen (Kontodaten), Gesundheitsdaten, …

Konsequenzen bzgl. der Daten: Was ist mit den Daten passiert bzw. kann passieren? Daten wurden vernichtet / gelöscht, Daten wurden verändert, Daten wurden unbefugt offengelegt / unrechtmäßig veröffentlicht

Auswirkungen auf Personen / die Universität: Welche Auswirkungen hat der Vorfall, bzw. könnte der Vorfall haben? (bspw. Prüfungsdaten des Bereichs … gelangten folgenden unberechtigten Personengruppen … innerhalb der Hochschule zur Kenntnis; Patentdaten wurden veröffentlicht, wodurch eine geplante Patentanmeldung durch die Universität gefährdet ist)

(Wahrscheinliche) Ursache: Was hat zu dem Fehler geführt? (bspw. menschlicher Fehler durch ungenaues Arbeiten, technisches Problem in der Applikation, Fehlkonfiguration / Sicherheitslücke durch fehlende Updates, die durch einen Hacker ausgenutzt wurde)

Bereits ergriffene Sofortmaßnahmen: Beschreibung der umgehend ausgeführten Sofortmaßnahmen um die Folgen des Vorfalls zu beschränken (z. B. Herunterfahren oder vom Netz nehmen des betroffenen Servers, Sperrung der Benutzer, die von falsch vergebenen Berechtigungen betroffen sind)

Weitere geplante / mögliche Maßnahmen: Welche weiteren Maßnahmen müssen getroffen werden, damit die Auswirkungen für die betroffenen Personen möglichst gering bleiben und der sichere Regelbetrieb wiederhergestellt werden kann? (bspw. Behebung des Programmfehlers und ausführliche Tests; Einspielen der aktuell veröffentlichten Sicherheitspatches …, Anschreiben der Personen, die unberechtigterweise Daten zu Kenntnis nehmen konnten, mit der Bitte diese zu Löschen und Inhalte vertraulich zu behandeln, künftige Nutzung eines sicheren Verschlüsselungs-verfahrens …)