Deutsche
Sporthochschule Köln
German Sport University Cologne

■ Am Sportpark Müngersdorf 6 ■ 50933 Köln ■

AMTLICHE MITTEILUNGEN

ze.IT

Nr.: 15/2020

Köln, den 23. Juni 2020

INHALT

Richtlinie zur Informationssicherheit

Konzept zur Steigerung der Sicherheit von Transport, Verarbeitung und Speicherung von Informationen an der DSHS Köln

---

Herausgeber: Der Rektor

1 Einleitung

Informationen sind essentielle Grundlage für eine erfolgreiche Arbeit in Forschung, Lehre und der Verwaltung einer Hochschule, weshalb sie angemessen geschützt werden müssen. Nahezu in allen Bereichen einer Hochschule basieren die relevanten Prozesse auf IT-Systemen, wodurch zum einen eine hohe Effizienz erreicht werden kann, zum anderen aber auch die Abhängigkeit einer unterbrechungsfreien System- und Dienst-Verfügbarkeit stetig zunimmt. Zusätzlich werden die Systeme im Kontext eines integrierten Informationsmanagements immer tiefer miteinander vernetzt.
Folglich ist es absolut erforderlich, die Risiken beim Einsatz der für ein integriertes Informationsmanagement benötigten Informationstechnischen Systeme zu erkennen, kontinuierlich zu analysieren und durch geeignete Maßnahmen zu minimieren.
Oberstes Ziel für die Deutsche Sporthochschule Köln (DSHS) ist es, die Verfügbarkeit von IT-Infrastruktur und -systemen, Daten und Diensten zu gewährleisten, die Vertraulichkeit zu schützen sowie die Integrität zu sichern. Dabei ist darauf zu achten, dass die Sicherheitsmaßnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der zu schützenden Informationen und der IT-Systeminfrastruktur stehen.

2 Geltungsbereich

Die Regelungen dieser Richtlinie gelten für Beschäftigte der DSHS. Gästen und sonstigen IT-Nutzer*innen wie beispielsweise Lehrbeauftragte, Dienstleister*innen, Mieter*innen, Pächter*innen gegenüber sind sie über die jeweiligen Nutzungs- oder Vertragsbedingungen einzubinden. Studierenden sind sie als Handlungsempfehlungen an die Hand zu geben.

3 Verantwortlichkeiten

Die Gesamtverantwortung für die Informationssicherheit / IT-Sicherheit liegt bei der Leitung der DSHS.

- Verantwortlich für Initiierung gemäß Bundesamt für Sicherheit in der Informationstechnik (BSI): Rektorat, IT-Sicherheitsbeauftragte*r
- Verantwortlich für Umsetzung gemäß BSI: IT-Sicherheitsbeauftragte*r
- Verantwortlich für die technische Umsetzung: Leitung der zentralen Betriebseinheit für Informationstechnologie (ze.IT)

4 Regelungen

4.1 Definition

Als IT-Sicherheitsvorfall wird an der DSHS ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit und / oder Integrität der digital gespeicherten Informationen und der betriebenen IT-Systeme und Anwendungen derart beeinträchtigt, dass ein großer Schaden für Forschung, Lehre und / oder Verwaltung der DSHS entstehen kann.

Definition der Informationssicherheitsschutzziele in Anlehnung an DIN ISO/IEC 27000:

- **Authentizität**[1]: Eigenschaft einer Einheit, das zu sein, was sie zu sein vorgibt.
- **Vertraulichkeit**[2]: Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.
- **Integrität**[3]**:** Eigenschaft der Richtigkeit und Vollständigkeit von Werten.
- **Verfügbarkeit**[4]: Eigenschaft, einer berechtigten Person oder Einheit auf Verlangen zugänglich und nutzbar zu sein.
- **Nicht-Abstreitbarkeit und Zurechenbarkeit**[5]: Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer Aktion und die verursachenden Einheiten nachzuweisen.
- **Verlässlichkeit**[6]: Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen.

Erläuterungen zu den Informationssicherheitsschutzzielen:

- **Authentizität** bedeutet, dass Daten jederzeit ihrem Ursprung zugeordnet werden können.
- **Vertraulichkeit** ist gewährleistet, wenn nur Personen, die dazu berechtigt sind, von schützenswerten Daten Kenntnis nehmen können.
- **Integrität** ist gewährleistet, wenn schützenswerte Daten unversehrt und vollständig bleiben.
- **Verfügbarkeit** bezieht sich auf Daten und Verfahren und bedeutet, dass sie zeitgerecht zur Verfügung stehen.
- **Nicht-Abstreitbarkeit** (Verbindlichkeit) bedeutet, dass es nicht möglich sein darf, ausgeführte Handlungen abzustreiten. Unter **Zurechenbarkeit** versteht man, dass es möglich sein muss, Handlungen eindeutig dem zuzuordnen, der sie ausgeführt hat.

[1] 3.6 authenticity in ISO/IEC 27000:2018(E)
[2] 3.10 confidentiality
[3] 3.36 integrity
[4] 3.7 availability
[5] 3.48 non-repudiation
[6] 3.55 reliability

4.2 CERT

Das Computer Emergency Response Team (CERT) besteht aus der / dem IT-Sicherheitsbeauftragten, den IT-Abteilungsleitungen sowie der Leitung von ze.IT.

Das CERT hat die Aufgabe, Informationssicherheitsvorfälle zu bewerten, geeignete Maßnahmen abzuwägen, zu beschließen und – bei Gefahr im Verzug – zu ergreifen.

4.3 Meldung

Sobald ein/e IT-Benutzer*in der DSHS etwas bemerkt, was er/sie für eine IT-sicherheitsrelevante Unregelmäßigkeit oder einen IT-Sicherheitsvorfall hält, muss er/sie diese/diesen schnellst möglich dem Helpdesk der DSHS melden. (siehe hierzu 4.1)

Der/Die IT-Benutzer*in informiert folglich umgehend den IT-Helpdesk der DSHS per E-Mail (support@dshs-koeln.de) oder per Telefon (+49 221 4982 6300).

4.4 Maßnahmen bei Vorfall der Informationssicherheit durch die zentrale Betriebseinheit für Informationstechnologie der DSHS Köln (ze.IT)

Nach Eingang der Meldung im IT-Helpdesk via E-Mail (support@dshs-koeln.de) oder per Telefon (+49 221 4982 6300) beginnt der / die diensthabende Beschäftigte während der Servicezeit, grundsätzlich vor Ablauf von vier Stunden, mit der Analyse und Bewertung der Meldung.

Schätzt der IT-Helpdesk den Vorfall als IT-Sicherheitsrelevant ein, wird eine erste, subjektive, Analyse der Schwere des Vorfalls vorgenommen. Analysiert wird die vermutliche Auswirkung auf die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Dienste und Daten der DSHS. Wird das Kritikalitätsniveau als gering eingestuft, so wird das CERT per E-Mail oder Telefon (Festnetz) informiert. Handelt es sich augenscheinlich um einen mittleren oder schwerwiegenden Vorfall, so wird das CERT schnellstmöglich, unter Nutzung aller verfügbaren Kommunikationswege informiert. Parallel werden, abhängig vom jeweiligen Problem, erste Maßnahmen ergriffen.

Das CERT kommt zusammen, wobei mindestens zwei Mitglieder benötigt werden, um beschlussfähig zu sein. Der/die IT-Sicherheitsbeauftragte*n leitet die CERT-Vorfallsitzung, ist er/sie nicht anwesend, leitet der / die höchstrangige (Eingruppierung, Dienstalter) Mitarbeiter*in die CERT-Vorfallsitzung.

Das CERT berät und ordnet den Vorfall abschließend ein. Es entscheidet, ob der IT-Vorfall tatsächlich sicherheitsrelevant ist. Wird dem Vorfall eine geringe Schwere zugeschrieben, so wird der Vorgang zur abschließenden Bearbeitung / Lösung zurück an den IT-Helpdesk gegeben. Wird dem Vorfall hingegen eine mittlere oder hohe Kritikalität zugeschrieben, ergreift das CERT alle erforderlichen unaufschiebbaren Maßnahmen zur Problembehebung und informiert unverzüglich die Hochschulleitung, und auch den / die IT-Sicherheitsbeauftragte*n sofern diese*r nicht anwesend war sowie – sofern personenbezogene Daten betroffen sein könnten – den oder die Datenschutzbeauftragte*n. Alle in Zusammenhang mit diesem Vorfall stehenden Maßnahmen und Informationsflüsse werden dokumentiert.

Abschließend wird die Gesamtdokumentation (BSI M06134) „Erfassung von IT-Sicherheitsvorfällen“ erstellt und im zentralen Ticketsystem der DSHS abgelegt.

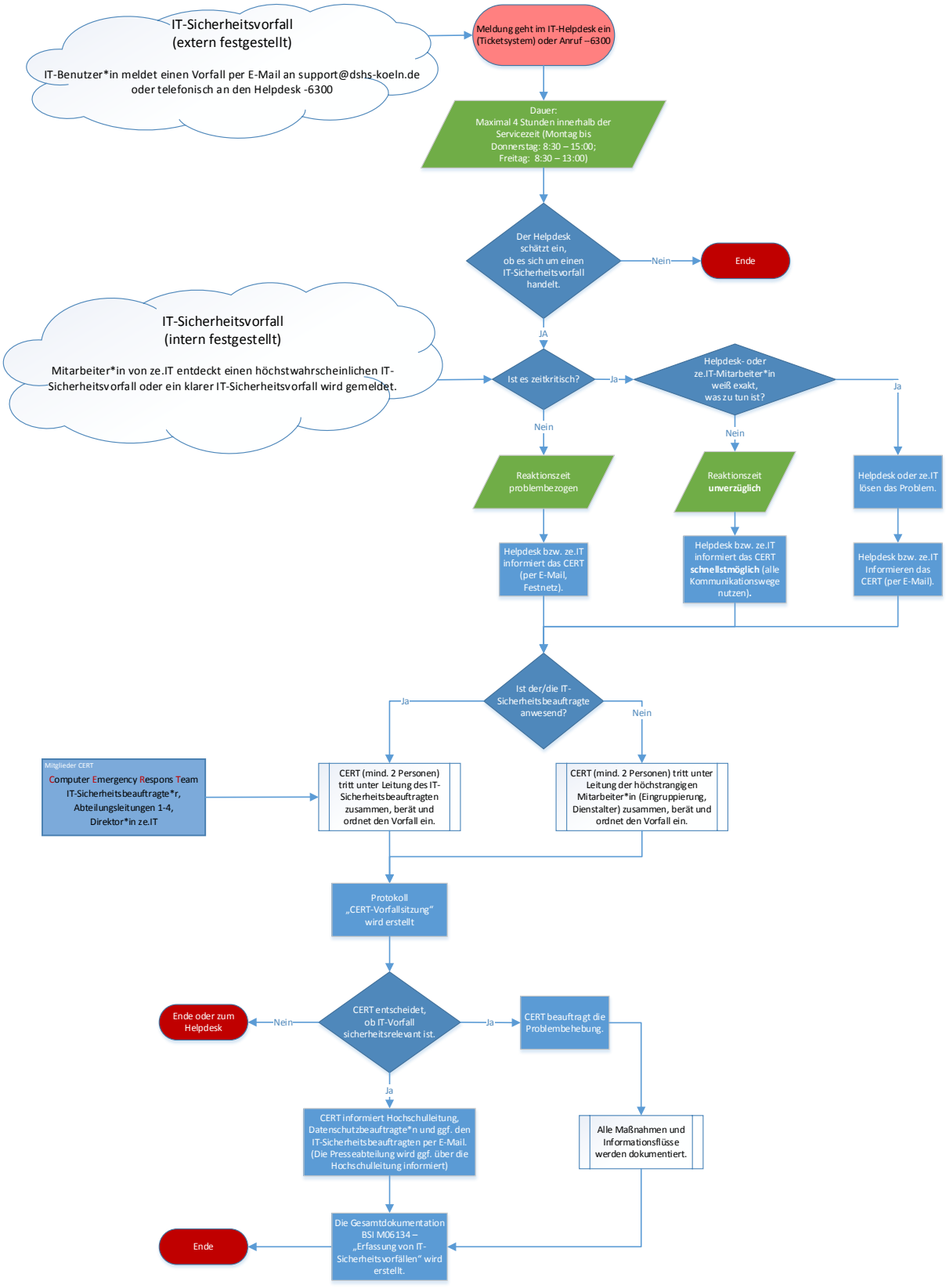


Abbildung 1: Informationssicherheitsprozess an der DSHS

4.5 Klassifizierung von Vorfällen der Informationssicherheit

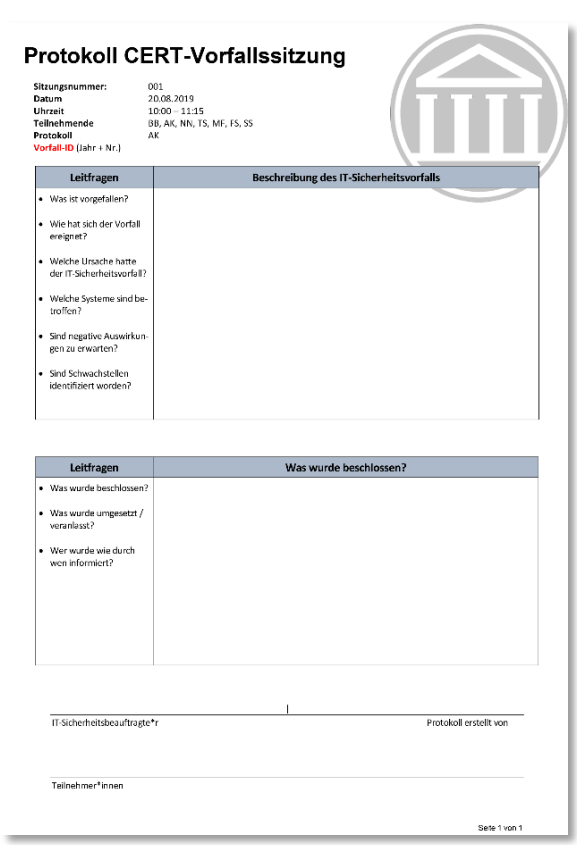
Um zu einer angemessenen Priorisierung einerseits und der als erforderlich identifizierten Maßnahmen andererseits zu gelangen, ist eine Analyse der Schwere eines Vorfalls erforderlich. Dazu wird das subjektive Maß „Schwere eines Vorfalls“ herangezogen, indem zu ermitteln ist, mit welchen wahrscheinlichen Auswirkungen auf die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Dienste und Daten der DSHS zu rechnen ist.

Art der Beeinträchtigung	**Schwere des IT-Sicherheitsvorfalls**		
	Niedrig	**Mittel**	**Hoch**
Beeinträchtigung der Aufgabenerfüllung	…führt maximal zum Ausfall **einzelner** Arbeitsabläufe (tolerierbare Ausfallzeit mehr als ein Arbeitstag).	…schränkt die Aufgabenerfüllung in einem **Teilbereich** ein (tolerierbare Ausfallzeit zwischen einer und 24 Stunden).	…gefährdet **insgesamt** die Arbeitsfähigkeit der DSHS (tolerierbare Ausfallzeit weniger als eine Stunde).
Negative Innen- / Außenwirkung	…führt höchstens zu einem **geringen** Ansehensverlust eines Teilbereichs der DSHS bei **Teilen** der Öffentlichkeit bzw. innerhalb der DSHS.	...führt zu einem Ansehens- und Vertrauensverlusts eines Teilbereichs der DSHS bei **größeren Teilen** der Öffentlichkeit bzw. innerhalb der DSHS.	...führt zu einem **großen** Ansehens- und Vertrauensverlust der DSHS in der **breiten** Öffentlichkeit sowie innerhalb der DSHS.
Finanzielle Auswirkungen	Geschätzte Summe der finanziellen Auswirkungen: **<= 10.000 €**	Geschätzte Summe der finanziellen Auswirkungen: **<= 200.000 €**	Geschätzte Summe der finanziellen Auswirkungen: **> 200.000 €**
Beeinträchtigung des Informationellen Selbstbestimmungsrechts (Datenschutz)	…hätte bei Missbrauch maximal **geringfügige** Auswirkungen auf die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse weniger Betroffener.	…hätte bei Missbrauch **erhebliche** Auswirkungen auf die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse der Betroffenen.	…hätte bei Missbrauch **gravierende** Auswirkungen auf die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse der Betroffenen. Oder es besteht Gefahr für Leib und Leben oder persönliche Freiheit.
Verstoß gegen Gesetze, Vorschriften und/oder Verträge	…führt zu **keinen** oder **geringen** Konsequenzen.	…führt zu **erheblichen** Konsequenzen.	…führt zu **gravierenden** Konsequenzen.
Beeinträchtigungen	**Niedrig**	**Mittel**	**Hoch**

Tabelle 1: Schwere des IT-Sicherheitsvorfalls

4.6 Dokumentation

Zur Dokumentation von Informationssicherheits- / IT-Sicherheitsvorfällen kommen zwei Formulare zum Einsatz. Zur Gewährleistung einer Nachvollziehbarkeit der Vorgänge und Beschlüsse im Rahmen der CERT-Vorfallsitzung kommt ein kompaktes Formular zum Einsatz. Zum Abschluss eines Vorfalls kommt das siebenseitige Formular „BSI – M06134“ zur Anwendung. Abgelegt werden beide Dokumente im zentralen Ticketsystem der DSHS.



Protokoll CERT-Vorfallssitzung

Sitzungsnummer: 001
Datum 20.08.2019
Uhrzeit 10:00 - 11:15
Teilnehmende BB, AK, NN, TS, MF, FS, SS
Protokoll AK
Vorfall-ID (Jahr + Nr.)

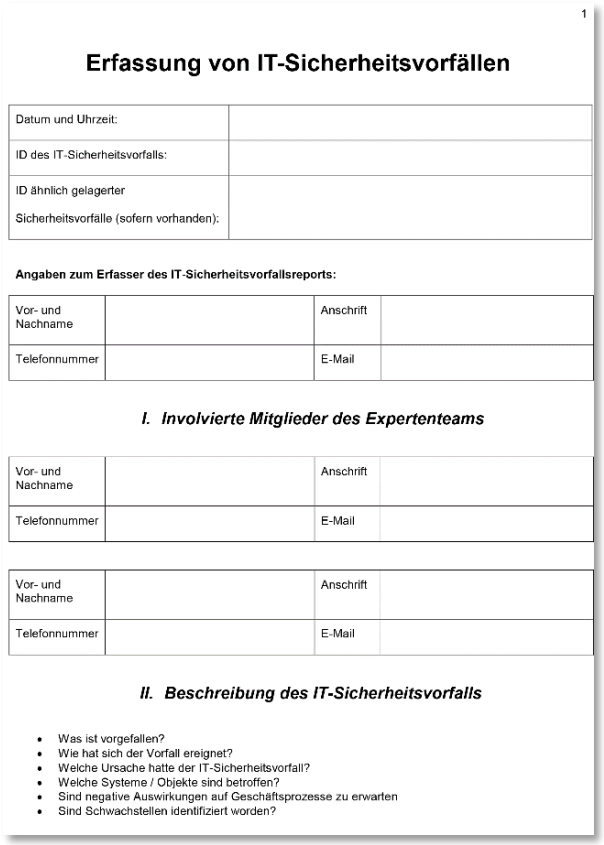
Leitfragen	Beschreibung des IT-Sicherheitsvorfalls
• Was ist vorgefallen? • Wie hat sich der Vorfall ereignet? • Welche Ursache hatte der IT-Sicherheitsvorfall? • Welche Systeme sind betroffen? • Sind negative Auswirkungen zu erwarten? • Sind Schwachstellen identifiziert worden?	

Leitfragen	Was wurde beschlossen?
• Was wurde beschlossen? • Was wurde umgesetzt / veranlasst? • Wer wurde wie durch wen informiert?	

IT-Sicherheitsbeauftragte*r — Protokoll erstellt von

Teilnehmer*innen

Seite 1 von 1



1

Erfassung von IT-Sicherheitsvorfällen

Datum und Uhrzeit:	
ID des IT-Sicherheitsvorfalls:	
ID ähnlich gelagerter Sicherheitsvorfälle (sofern vorhanden):	

Angaben zum Erfasser des IT-Sicherheitsvorfallsreports:

Vor- und Nachname		Anschrift	
Telefonnummer		E-Mail	

I. Involvierte Mitglieder des Expertenteams

Vor- und Nachname		Anschrift	
Telefonnummer		E-Mail	

Vor- und Nachname		Anschrift	
Telefonnummer		E-Mail	

II. Beschreibung des IT-Sicherheitsvorfalls

- Was ist vorgefallen?
- Wie hat sich der Vorfall ereignet?
- Welche Ursache hatte der IT-Sicherheitsvorfall?
- Welche Systeme / Objekte sind betroffen?
- Sind negative Auswirkungen auf Geschäftsprozesse zu erwarten
- Sind Schwachstellen identifiziert worden?

5 Revision

Diese Richtlinie wird regelmäßig, jedoch mindestens einmal pro Jahr, durch den oder die Informationssicherheitsbeauftragte / IT-Sicherheitsbeauftragte auf ihre Aktualität und Konformität mit den Informationssicherheitsregelungen der DSHS überprüft.

6 Inkrafttreten

Diese Richtlinie tritt am Tage nach ihrer Veröffentlichung in den Amtlichen Mitteilung der Deutschen Sporthochschule Köln in Kraft.

Ausgefertigt aufgrund des Beschlusses des Rektorats der Deutschen Sporthochschule Köln vom 02.03.2020.

Köln, 23. Juni 2020

Der Rektor der Deutschen Sporthochschule Köln

Univ.-Prof. Dr. Heiko Strüder