

Akkreditierungsurkunde

Der Studiengang

Cyber Security

Master of Engineering (M.Eng.)

hat das interne Verfahren zur Qualitätssicherung mit Erfolg durchlaufen. Die Akkreditierung erfolgte durch ein Internes Audit, welches mit der Verleihung des Siegels des Akkreditierungsrates abschließt.

Die Technische Hochschule Deggendorf ist seit dem 09.09.2020 durch die Akkreditierungsagentur ASIIN systemakkreditiert und damit berechtigt, die Qualität ihrer Studiengänge anhand der European Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG), des Qualifikationsrahmens für deutsche Hochschulabschlüsse und den Vorgaben aus dem Studienakkreditierungsstaatsvertrag in Verbindung mit der Bayerischen Studienakkreditierungsverordnung (BayStudAkkV) selbst zu prüfen und zu akkreditieren.

Der Beschluss über die Akkreditierung erfolgt auf Basis der Ergebnisse des Internen Audits und der vorgeschlagenen Auflagen, Empfehlungen und Hinweise durch das Auditierungsgremium.

Die Akkreditierung wurde am 05.03.2026 vom internen Akkreditierungsgremium unter Auflagen beschlossen und ist vorläufig bis zum 05.03.2027 befristet.

Nach Aufлагenerfüllung gilt die Akkreditierung bis zum 05.03.2034.



Deggendorf, 05.03.2026


Prof. Waldemar Berg
Präsident

Kurzbeschreibung des Verfahrens

Die internen Akkreditierungen (= Interne Audits) finden alle acht Jahre statt. Die Gutachtergruppen setzen sich aus jeweils mindestens vier Personen aus verschiedenen Bereichen zusammen, was eine umfassende Einschätzung der Qualität eines Studiengangs sicherstellt:

- Mindestens zwei externe professorale Vertreterinnen oder Vertreter von Hochschulen und / oder Universitäten
- Mindestens eine Vertreterin oder ein Vertreter der Berufspraxis, Industrie- oder Unternehmensvertreterin oder Unternehmensvertreter
- Mindestens eine Vertreterin oder ein Vertreter der Studierenden, die oder der im Moment den gleichen bzw. einen ähnlichen Studiengang an einer anderen Hochschule bzw. Universität studiert oder vor kurzem abgeschlossen hat.

Die Begutachtung der formalen Akkreditierungsanforderungen und hochschulrechtlichen Vorgaben erfolgt bereits vorab im Rahmen der formellen Prüfung des Studiengangs durch das ZQM, wird aber mit den Gutachterinnen und Gutachtern nochmal aufgegriffen.

Die Überprüfung der für den jeweiligen Studiengang erforderlichen personellen und sächlich-räumlichen Ressourcen erfolgt durch die zuständige Fakultät, wird aber am Audittag auch nochmal aufgegriffen, um den Gesamteindruck des Studiengangs zu bewerten. Darüber hinaus bewerten die Verantwortlichen der Fakultät sowohl die fachlich-inhaltlichen als auch die formellen Kriterien innerhalb eines Selbstaudits und füllen eine Fakultätscheckliste aus.

Der Audittag ist so gestaltet, dass vom ZQM gezielt auf die Fragen und Bemerkungen eingegangen wird, welche die Gutachterinnen und Gutachter im Vorfeld bei einer Online-Befragung mit EvaSys beschrieben haben. Hierzu wurde den Gutachterinnen und Gutachtern eine Checkliste zur Verfügung gestellt, die die relevanten Punkte der BayStudAkkV abdeckt. Im Fokus steht eine fachlich-inhaltliche Bewertung des Studiengangs und des zugrunde gelegten Konzepts anhand der Gesamtdokumentation, die per Cloud geteilt wird.

Damit eine ganzheitliche Bewertung des Studiengangs möglich ist, sind bei einem Internen Audit Befragungen von Lehrenden und Studierenden des Studiengangs vorgesehen.

Die Internen Audits dienen zur Überprüfung, ob diese Prozesse auf der Ebene des Studiengangs umgesetzt und „gelebt“ werden. Die Verfahren weisen einen hohen Beratungscharakter auf und sind von einer großen Offenheit und gegenseitigem Respekt geprägt.

Zwischen zwei Audits, also nach vier Jahren, wird eine kleine Überprüfung des Studiengangs (= Internes Review) vorgenommen, um festzustellen, ob das Studiengangskonzept inkl. Qualifikationsprofil noch aktuell ist oder ob Verbesserungsbedarf besteht. Auch bei einem Internen Review wird der Studiengang gemeinsam mit Industrievertreterinnen und -vertretern, Vertreterinnen und Vertretern der Berufspraxis, Lehrenden und Studierenden bzw. Absolventinnen und Absolventen auf Aktualität und Adäquanz der Inhalte überprüft und ein Protokoll über mögliche Maßnahmen erstellt. Eine Umsetzung wird beim nächsten Internen Audit überprüft.

Kurzprofil des Studiengangs

Hochschule	Technische Hochschule Deggendorf			
Ggf. Standort	Campus Deggendorf			
Studiengang (Name/Bezeichnung) ggf. inkl. Namensänderungen	Cyber Security			
Abschlussgrad / Abschlussbezeichnung	Master of Engineering (M.Eng.)			
Studienform	Präsenz	☒	Blended Learning	☒
	Vollzeit	☐	Intensiv	☐
	Teilzeit	☒	Joint Degree	☐
	Dual	☐	Lehramt	☐
	Berufsbegleitend	☒	Kombination	☐
	Fernstudium	☐	Double Degree	☐
Regelstudienzeit (in Semestern)	5			
Zulassungsvoraussetzungen	Abgeschlossenes Erststudium aus dem Bereich der Ingenieurwissenschaften oder Informatik an einer anerkannten Hochschule Erfolgreiches Durchlaufen des Bewerbungsverfahrens inkl. eines Orientierungsgesprächs mit dem Studiengangsleiter			
Anzahl der vergebenen ECTS-Punkte	90			
Unterrichtssprache	Deutsch			
Kooperationen (studiengangsbezogen)	-			
Studienbeginn	Wintersemester			
Anzahl Studienanfänger pro Semester	ca. 8 Anfänger			
Studiengangskoordinator	Prof. Dr.-Ing. Andreas Grzempa			

Die Sicherheit von IT-Systemen steht zunehmend im Fokus. Dabei gibt es im Bereich IT-Security nur wenige berufsbegleitende Masterstudiengänge, welche umfassend und zugleich mit speziellen Vertiefungsrichtungen die Experten von Morgen qualifizieren. Der Master „Cyber Security“ ist in Deutschland einer der wenigen berufsbegleitend absolvierbaren IT Security Studiengänge, welcher eine holistische Qualifizierung in diesem Bereich ermöglicht. Der Studiengang richtet sich an Absolventinnen und Absolventen aus dem Bereich Ingenieurwissenschaften oder Informatik, die ihr Fachwissen im Bereich IT Security vertiefen möchten. Besonderes Gewicht wird auf die Anwendung von Security Technologien im Kontext von Industrie 4.0, bei kritischen Infrastrukturen und beim Autonomen Fahren gelegt.

Die Studierenden besitzen nach Abschluss des berufsbegleitenden Masterstudienganges „Cyber Security“ die Fähigkeit, Bedrohungen und Gefahren für individuelle Anwendungsfälle zu erkennen und zu formulieren, das resultierende Risiko zu analysieren sowie selbstständig geeignete Sicherheitsstrategien zu erarbeiten und umzusetzen. Weiter sind die Studierenden durch das vermittelte Wissen des berufsbegleitenden Masterstudienganges „Cyber Security“ in der Lage, Sicherheitsvorfälle in den Bereichen Industrial und Automotive zu erkennen und darzustellen, was sowohl bei forensischen Untersuchungen als auch beim Informationssicherheitsmanagement unerlässlich ist.

Durch heterogene Studiengruppen werden die Studierenden auf ihr späteres Arbeitsleben im Unternehmen vorbereitet. In den Semestern zwei und vier vertiefen die Studierenden ihr Fachwissen in den Bereichen Industrial und Automotive IT Security. Im Besonderen werden den Teilnehmerinnen und Teilnehmern auch fachübergreifende und internationale Kenntnisse nähergebracht, die sie in die Lage versetzen, Gesamtsysteme und -prozesse zu überschauen. Durch diesen ganzheitlichen Ansatz können Absolventen Probleme nicht nur aus einer fachspezifischen Sicht beurteilen, sondern können den Gesamtnutzen für das Unternehmen optimieren.

Gutachtergruppe beim Internen Audit Master „Cyber Security“ am 09.01.2026:

- FH-Prof. DI Robert Kolmhofer: Professor und Studiengangleiter des Masters „Sichere Informationssysteme“ am Campus Hagenberg der Fachhochschule Oberösterreich
- FH Prof. Dr. Simon Tjoa: Professor und Studiengangsleiter des Masters „Cyber Security and Resilience“ an der Fachhochschule St. Pölten
- Dr.-Ing. Ugur Akcakoca: Vertreter der Berufspraxis
- Philipp Schrefel: Student im Master „Sichere Informationssysteme“ am Campus Hagenberg der Fachhochschule Oberösterreich

Beschlussempfehlung des Gutachterteams:

Auf Basis der eingereichten, studiengangsspezifischen Unterlagen und der Dokumentation des Internen Audits haben die Gutachter festgestellt:

	Ja	Nein
Die formalen Kriterien sind erfüllt.	☐	☒
Die fachlich-inhaltlichen Kriterien sind erfüllt.	☐	☒

Auflagen, Empfehlungen und Hinweise des Gutachterteams zur Weiterentwicklung des Masterstudiengangs „Cyber Security“:

Auflagen:

Auflage zum Prüfpunkt Modularisierung, Punkt 15: *„Alle Module des Studiengangs sind im Modulhandbuch der Fakultät beschrieben und enthalten die vorgegeben Inhalte als Mindestanforderung (a-i). Darüber hinaus sind Angaben zu Literaturempfehlungen und zur Gewichtung des Moduls in den Modulbeschreibungen enthalten“:*

1. Die Literaturquellen im Modulhandbuch müssen aktualisiert werden.

Auflage zum Prüfpunkt fachlich-inhaltliche Gestaltung der Studiengänge, Punkt 32: *„Die Aktualität und Adäquanz der fachlichen und wissenschaftlichen Anforderungen ist gewährleistet“:*

2. Die Richtlinien zur Nutzung von KI müssen den Studierenden zu Beginn des Studiums zur Verfügung gestellt werden.

Empfehlung:

Empfehlung zum Prüfpunkt Berufsbefähigung, Punkt 36: *„Es wird dargelegt, für welche Berufsfelder und Tätigkeiten die Absolventen ausgebildet werden“:*

3. Das Dokument zu den Berufsfeldern von Absolventinnen und Absolventen sollte konkretisiert und überarbeitet werden.

Hinweise:

Hinweis zum Prüfpunkt Modularisierung, Punkt 15: *„Alle Module des Studiengangs sind im Modulhandbuch der Fakultät beschrieben und enthalten die vorgegeben Inhalte als Mindestanforderung (a-i). Darüber hinaus sind Angaben zu Literaturempfehlungen und zur Gewichtung des Moduls in den Modulbeschreibungen enthalten“* und Prüfpunkt Qualifikationsziele und Abschlussniveau, Punkt 16: *„Die Qualifikationsziele und die angestrebten Lernergebnisse sind klar formuliert“:*

4. In den Qualifikationszielen des Studiengangs sowie den Modulbeschreibungen könnten die jeweiligen Bloom'schen Taxonomiestufen explizit erwähnt werden. Zudem könnte darauf geachtet werden, dass die vermittelten sozialen Kompetenzen noch stärker hervorgehoben werden.

Hinweis zum Prüfpunkt Schlüssiges Studiengangskonzept und adäquate Umsetzung, Punkt 24: *„Die studentische Mobilität wird, wo möglich, gefördert. Es werden Rahmenbedingungen geschaffen, um den Studierenden einen Aufenthalt an anderen Hochschulen ohne Zeitverlust zu ermöglichen“:*

5. Mögliche Mobilitätsfenster im Studiengang könnten konkret beschrieben werden (z.B. über die Homepage).

Beschluss des internen Akkreditierungsgremiums an der Technischen Hochschule Deggendorf vom 05.03.2026:

Das Akkreditierungsgremium hat am 05.03.2026 beschlossen, den berufsbegleitenden Masterstudiengang „Cyber Security“ mit den Auflagen, Empfehlung und Hinweisen des Gutachterteams zu akkreditieren. Der Studiengang wurde im Verfahren anhand der Mindestanforderungen geprüft.

Ergebnis:

	Ja	Nein
Die formalen Kriterien sind erfüllt.	☐	☒
Die fachlich-inhaltlichen Kriterien sind erfüllt.	☐	☒

Das Akkreditierungsgremium spricht für den Masterstudiengang „Cyber Security“ (M.Eng.) eine Verleihung des Siegels des Akkreditierungsrates bis zum 05.03.2034 mit zwei Auflagen, einer Empfehlung und zwei Hinweisen aus. Die Auflagen sind bis zum 05.03.2027 zu erfüllen.

Auflagenerfüllung:

Die Auflagen sind bis zum 05.03.2027 zu erfüllen.