

Ergebnisbericht zum Verfahren zur Akkreditierung des FH- Masterstudiengangs „Cyber Security and Resilience“, StgKz A0863, der Fachhochschule St.Pölten, durchgeführt in St.Pölten

1 Antragsgegenstand

Die Agentur für Qualitätssicherung und Akkreditierung Austria (AQ Austria) führte ein Verfahren zur Akkreditierung des FH-Masterstudiengangs „Cyber Security and Resilience“, StgKz A0863, der Fachhochschule St.Pölten, durchgeführt in St.Pölten, gem § 23 Abs 3 (Inst.Akk) / 4 (Progr. akkr) / § 26 Abs 1 Z 1 (Reakk) Hochschul-Qualitätssicherungsgesetz (HS-QSG), BGBl I Nr. 74/2011 idgF, iVm § 8 Fachhochschul-Studiengesetz (FHStG) BGBl. Nr. 340/1993 idgF und iVm § 17 Fachhochschul-Akkreditierungsverordnung 2019 (FH-AkkVO) durch. Gem § 21 HS-QSG veröffentlicht die AQ Austria folgenden Ergebnisbericht:

2 Verfahrensablauf

Das Akkreditierungsverfahren umfasste folgende Verfahrensschritte:

Verfahrensschritt	Zeitpunkt
Antrag eingelangt am	19.12.2019
Rückmeldung der Geschäftsstelle zum Antrag an Antragstellerin	14.02.2020
Überarbeiteter Antrag eingelangt am	26.02.2020



Mitteilung an Antragstellerin Abschluss der Prüfung des Antrags durch die Geschäftsstelle	19.03.2020
Bestellung der Gutachter/innen	17.04.2020
Information Antragstellerin über Gutachter/innen	17.04.2020
Erstes virtuelles Vorbereitungsgespräch mit Gutachter/innen	28.04.2020
Zweites virtuelles Vorbereitungsgespräch mit Gutachter/innen	13.05.2020
Fragenkatalog der Gutachter/innen an Antragstellerin	06.05.2020
Antworten auf den Fragenkatalog durch Antragstellerin	11.05.2020
Nachreichungen in Bezug auf Fragenkatalog	11.05.2020
Virtuelles Gespräch der Vertreter/innen der Antragsteller/in und den Gutachter/innen	14.05.2020
Nachreichungen nach virtuellem Gespräch mit den Vertreter/innen der Antragsteller/in	19.05.2020
Vorlage des Gutachtens	20.06.2020
Gutachten an Antragstellerin zur Stellungnahme	22.06.2020
Kostenaufstellung an Antragstellerin zur Stellungnahme	22.06.2020
Stellungnahme Antragstellerin zum Gutachten	25.06.2020
Stellungnahme Antragstellerin zur Kostenaufstellung	23.06.2020
Stellungnahme Antragstellerin zum Gutachten an Gutachter/innengruppe	25.06.2020

3 Akkreditierungsentscheidung

Das Board der AQ Austria hat in seiner 61. Sitzung am 29.06.2020 entschieden, dem Antrag auf Akkreditierung des FH-Masterstudiengangs „Cyber Security and Resilience“, StgKz A0863, der FH St.Pölten, durchgeführt in St.Pölten stattzugeben.

Die Entscheidung wurde am 17.07.2020 vom zuständigen Bundesminister genehmigt. Die Entscheidung ist seit 17.07.2020 rechtskräftig.



4 Anlage/n

- Gutachten vom 20.06.2020
- Stellungnahme vom 25.06.2020

AQ Austria, 1190 Wien, Franz-Klein-Gasse 5



Agentur für
Qualitätssicherung
und Akkreditierung
Austria

Gutachten zum Verfahren zur Akkreditierung des FH-Masterstudiengangs „Cyber Security and Resilience“, A0863 der Erhalterin FH St. Pölten, durchgeführt in St. Pölten

gem § 7 der Fachhochschul-Akkreditierungsverordnung 2019 (FH-AkkVO)

Wien, 22.06.2020

Inhaltsverzeichnis

1	Verfahrensgrundlagen	6
2	Kurzinformation zum Akkreditierungsverfahren	8
3	Vorbemerkungen der Gutachter/innen	9
4	Begutachtung und Beurteilung anhand der Beurteilungskriterien der FH-AkkVO . 9	
4.1	Beurteilungskriterium § 17 Abs 1 Z 1–2: Entwicklung und Qualitätssicherung des Studiengangs.....	9
4.2	Beurteilungskriterium § 17 Abs 2 Z 1–12: Studiengang und Studiengangsmanagement	10
4.3	Beurteilungskriterium § 17 Abs 3 Z 1–7: Personal.....	16
4.4	Beurteilungskriterium § 17 Abs 4: Finanzierung.....	19
4.5	Beurteilungskriterium § 17 Abs 5: Infrastruktur.....	20
4.6	Beurteilungskriterium § 17 Abs 6 Z 1–2: Angewandte Forschung und Entwicklung..	20
4.7	Beurteilungskriterium § 17 Abs 7: Kooperationen	22
5	Zusammenfassung und abschließende Bewertung	23
6	Eingesehene Dokumente	24

5 Verfahrengrundlagen

Das österreichische Hochschulsystem

Das österreichische Hochschulsystem umfasst derzeit:

- 22 öffentliche Universitäten; darunter die Donau-Universität Krems, eine Universität für postgraduale Weiterbildung;
- 16 Privatuniversitäten, erhalten von privaten Trägern mit staatlicher Akkreditierung;
- 21 Fachhochschulen, erhalten von privatrechtlich organisierten und staatlich subventionierten oder von öffentlichen Trägern mit staatlicher Akkreditierung;
- die Pädagogischen Hochschulen, erhalten vom Staat oder von privaten Trägern mit staatlicher Akkreditierung;
- die Philosophisch-Theologischen Hochschulen, erhalten von der Katholischen Kirche;
- das Institute of Science and Technology Austria, dessen Aufgaben in der Erschließung und Entwicklung neuer Forschungsfelder und der Postgraduiertenausbildung in Form von PhD-Programmen und Post Doc-Programmen liegt.

Im Wintersemester 2019/20¹ studieren 268.586 Studierende an öffentlichen Universitäten (inkl. der Donau-Universität Krems). Weiters sind 53.401 Studierende an Fachhochschulen und 15.063 Studierende an Privatuniversitäten eingeschrieben.

Externe Qualitätssicherung

Öffentliche Universitäten müssen gemäß Hochschul-Qualitätssicherungsgesetz (HS-QSG) alle sieben Jahre ihr internes Qualitätsmanagementsystem in einem Auditverfahren zertifizieren lassen. An die Zertifizierungsentscheidungen sind keine rechtlichen oder finanziellen Konsequenzen gekoppelt.

Privatuniversitäten müssen sich alle sechs Jahre von der AQ Austria institutionell akkreditieren lassen. Nach einer ununterbrochenen Akkreditierungsdauer von zwölf Jahren kann die Akkreditierung auch für zwölf Jahre erfolgen. Zwischenzeitlich eingerichtete Studiengänge und Lehrgänge, die zu akademischen Graden führen, unterliegen ebenfalls der Akkreditierungspflicht.

Fachhochschulen müssen sich nach der erstmaligen institutionellen Akkreditierung nach sechs Jahren einmalig reakkreditieren lassen, dann gehen auch die Fachhochschulen in das System des Audits über, wobei der Akkreditierungsstatus an eine positive Zertifizierungsentscheidung im Auditverfahren gekoppelt ist. Studiengänge sind vor Aufnahme des Studienbetriebs einmalig zu akkreditieren.

Akkreditierung von Fachhochschul-Einrichtungen und ihren Studiengängen

Fachhochschulen bedürfen in Österreich einer einmalig zu erneuernden institutionellen Akkreditierung, um als Hochschulen tätig sein zu können. Neben dieser institutionellen Akkreditierung sind auch die Studiengänge der Fachhochschulen vor Aufnahme des Studienbetriebs einmalig zu akkreditieren. Für die Akkreditierung ist die AQ Austria zuständig.

¹ Stand Februar 2020, Datenquelle Statistik Austria/unidata/BMBWF. Im Gegensatz zu den Daten der öffentlichen Universitäten sind im Fall der Fachhochschulen in Studierendenzahlen jene der außerordentlichen Studierenden nicht enthalten. An den öffentlichen Universitäten studieren im WS 2018/19 278.039 ordentliche Studierende.



Die Akkreditierungsverfahren werden nach der Fachhochschul-Akkreditierungsverordnung 2019 (FH-AkkVO)² der AQ Austria durchgeführt. Im Übrigen legt die Agentur ihren Verfahren die Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG)³ zugrunde.

Für die Begutachtung von Akkreditierungsanträgen bestellt die AQ Austria Gutachter/innen. Diese erstellen auf Basis der Antragsunterlagen und eines Vor-Ort-Besuchs bei der antragstellenden Institution ein gemeinsames schriftliches Gutachten. Anschließend trifft das Board der AQ Austria auf der Grundlage des Gutachtens und unter Würdigung der Stellungnahme der Hochschule die Akkreditierungsentscheidung. Bei Vorliegen der gesetzlichen Akkreditierungsvoraussetzungen und Erfüllung der geforderten qualitativen Anforderungen werden die Studiengänge mit Bescheid akkreditiert.

Der Bescheid des Boards bedarf vor Inkrafttreten der Genehmigung durch den zuständigen Bundesminister. Nach Abschluss des Verfahrens werden jedenfalls ein Ergebnisbericht über das Verfahren und das Gutachten auf der Website der AQ Austria und der Website der Antragstellerin veröffentlicht. Ausgenommen von der Veröffentlichung sind personenbezogene Daten und jene Berichtsteile, die sich auf Finanzierungsquellen sowie Geschäfts- und Betriebsgeheimnisse beziehen.

Bei Anträgen aus den Ausbildungsbereichen der gehobenen medizinisch-technischen Dienste, der Hebammen sowie der allgemeinen Gesundheits- und Krankenpflege sind bei der Bestellung der Gutachter/innen die gem § 3 Abs 6 Bundesgesetz über die Regelung der gehobenen medizinisch-technischen Dienste (MTD-Gesetz), § 11 Abs 4 Bundesgesetz über den Hebammenberuf (HebG) und § 28 Abs 4 Bundesgesetz über Gesundheits- und Krankenpflegeberufe (GuKG) durch das Bundesministerium für Gesundheit nominierten Sachverständigen beizuziehen. Die AQ Austria hat bei der Entscheidung über Anträge auf Akkreditierung, Verlängerung oder bei Widerruf der Akkreditierung von Fachhochschul-Bachelorstudiengängen für die Ausbildung in den gehobenen medizinisch-technischen Diensten, der Hebammen sowie der allgemeinen Gesundheits- und Krankenpflege das Einvernehmen des Bundesministers/der Bundesministerin für Gesundheit einzuholen.

Rechtliche Grundlagen für die Akkreditierung von Fachhochschulstudiengängen sind das Hochschul-Qualitätssicherungsgesetz (HS-QSG)⁴ sowie das Fachhochschul-Studiengesetz (FHStG)⁵.

² Fachhochschul-Akkreditierungsverordnung 2019

³ Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG)

⁴ Hochschul-Qualitätssicherungsgesetz (HS-QSG)

⁵ Fachhochschulstudiengesetz (FHStG)

6 Kurzinformation zum Akkreditierungsverfahren

Information zur antragstellenden Einrichtung	
Antragstellende Einrichtung	Erhalterin FH St.Pölten
Rechtsform	Gesellschaft mit beschränkter Haftung
Standort	St. Pölten
Anzahl der Studierenden	3 219 (Stand 15.11.2018)
Informationen zum Antrag auf Akkreditierung	
Studiengangsbezeichnung	Cyber Security and Resilience
Studiengangsart	Masterstudiengang
ECTS-Punkte	120
Regelstudiodauer	4 Semester
Anzahl der Studienplätze	30
Akademischer Grad	Master of Science in Engineering (MSc)
Organisationsform	Vollzeit/ Duales Studium
Verwendete Sprache	Englisch
Ort der Durchführung	St. Pölten
Studienbeitrag	363,36 €

Die Erhalterin reichte am 19.12.2019 den Akkreditierungsantrag ein. Mit Beschluss vom 17.04.2020 bestellte das Board der AQ Austria folgende Gutachter/innen für die Begutachtung des Antrags:

Name	Institution	Rolle in der Gutachter/innengruppe
Prof. Dr. Gabi Dreo Rodosek	Universität der Bundeswehr München	Gutachterin mit wissenschaftlicher und berufspraktischer Qualifikation; Vorsitzende der Gutachter/innengruppe
Prof. Sarah Hauser	Fachhochschule Nordwestschweiz	Gutachterin mit wissenschaftlicher und berufspraktischer Qualifikation
DDr. Florian Skopik	AIT Austrian Institute of Technology GmbH	Gutachter mit berufspraktischer und wissenschaftlicher Qualifikation
Stefan Buschbeck , BSc	FH Campus Wien	Studentischer Gutachter

Am 14.05.2020 fanden Online-Gespräche der Gutachter/innen und der Vertreter/innen der AQ Austria mit der Erhalterin statt.

7 Vorbemerkungen der Gutachter/innen

Die Bedeutung der Informations und Kommunikationstechnologie ist enorm - sie ist das Rückgrat unserer modernen digitalen Gesellschaft und Wirtschaft. Daher ist es essentiell, IKT-gestützte Systeme widerstandsfähig gegenüber Cyber Angriffen zu machen. Um dies zu bewerkstelligen, müssen künftig noch mehr Fachkräfte ausgebildet werden, die solche Systeme entwerfen, aufbauen und betreiben. Der neue Masterstudiengang „Cyber Security and Resilience“ an der FH St. Pölten hat genau dies zum Ziel. Das Gutachterteam konnte sich auf Basis eines detailliert ausgearbeiteten Antrags schon vor den persönlichen Gesprächen mit dem Entwicklungsteam der FH ein gutes Bild vom beantragten Studiengang machen. Der übliche Vor-Ort-Besuch wurde bedingt durch die Covid19-Umstände durch eine Videokonferenz ersetzt. Diese war gut organisiert. Dem Gutachterteam standen in verschiedenen Gesprächsrunden unterschiedliche Gruppen (Leitung der Fachhochschule St. Pölten, Entwicklungsteam, Lehrende und Studierende) zur Beantwortung der Fragen zur Verfügung. Alle Gespräche fanden in professionell freundlicher Atmosphäre statt. Es blieben keine Fragen unbeantwortet.

8 Begutachtung und Beurteilung anhand der Beurteilungskriterien der FH-AkkVO

8.1 Beurteilungskriterium § 17 Abs 1 Z 1–2: Entwicklung und Qualitätssicherung des Studiengangs

Entwicklung und Qualitätssicherung des Studiengangs

1. Der Studiengang wurde mit einem definierten Prozess zur Entwicklung und Einrichtung von Studiengängen entwickelt, in den die relevanten Interessengruppen eingebunden waren.

Der Studiengang "Cyber Security and Resilience" wurde anhand eines definierten Prozesses zur Entwicklung und Einrichtung von Studiengängen entwickelt, in dem alle relevanten Stakeholder eingebunden waren. Strategisch gesehen verstärkt der neue Studiengang das Profilelement IT-Sicherheit der FH St. Pölten, um den enormen Bedarf an Cybersecurity-Spezialisten zu adressieren. Der neue Studiengang komplementiert mit sehr viel Synergiepotential die vorhandenen Studiengänge, liefert Forschungsimpulse für andere Departments und spricht durch die englischsprachige Ausrichtung internationale Studierende an.

Das Entwicklungsteam bestand aus drei Personen mit ausgewiesener wissenschaftlicher Qualifikation sowie 25 Personen, die über die für den Studiengang relevante Berufstätigkeit verfügten. Zwei weitere Mitglieder haben ihre Kompetenzen im Hinblick auf die Studiengangsentwicklung sowie Didaktik und innovative Lehr- und Lernformate eingebracht. Einige Mitglieder der Entwicklungsteams werden aktiv die Lehrveranstaltungen des neuen Studiengangs unterstützen. Die Zusammensetzung des Entwicklungsteams verdeutlicht sehr gut, dass alle notwendige Kompetenz an der Entwicklung des Studiengangs mitgewirkt hat.

Der Akkreditierungsantrag wurde durch den Ausschuss für Programmentwicklung der FH St. Pölten begutachtet. Im Ausschuss sind Department- und StudiengangsleiterInnen, MitarbeiterInnen aus der FH-Serviceabteilungen und Studierende vertreten. Neben dem Ausschuss für Programmentwicklung sind Studierende auch im Ausschuss für die

Qualitätsentwicklung der Lehre vertreten. Damit ist gewährleistet, dass alle relevanten Stakeholder aktiv an der Entwicklung des Studiengangs beteiligt sind.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Empfehlung:

Das Gutachterteam empfiehlt die Stärken des neuen Studiengangs konsequent hervorzuheben, um den Studierenden sowohl fundiertes IT-Sicherheitswissen zu vermitteln als auch diese auf die zukünftigen Managementaufgaben vorzubereiten.

Entwicklung und Qualitätssicherung des Studiengangs

2. Der Studiengang ist nach erfolgter Akkreditierung in das Qualitätsmanagementsystem der Fachhochschul-Einrichtung eingebunden.

Der Studiengang ist nach erfolgreicher Akkreditierung in das Qualitätsmanagement der Fachschule eingebunden. Das QM-System der FH St. Pölten ist sehr differenziert und umfasst alle Leistungsbereiche der Hochschule mit besonderem Fokus auf Studium und Lehre. Es beinhaltet u.a. regelmäßige externe Evaluierung der FH, Evaluierungszyklen, strukturiertes internes und externes Berichtswesen, transparentes Set an Daten und Kennzahlen. Eine Auflistung der Einbindung des Studiengangs in die Qualitätssicherungsinstrumente, wie z.B. das Dokumentationsverfahren und interne Plattformen zur Prozessdarstellung, in denen Ergebnisse interner und externer Qualitätssicherungsmaßnahmen, laufende Kennzahlen und Qualitätsberichte für verschiedene Stakeholder zusammengefasst sind, ist detailliert dargelegt. Die Teilnahme an nationalen und internationalen Benchmarkings ist ein weiteres Instrument des Qualitätssicherungsprozesses.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

8.2 Beurteilungskriterium § 17 Abs 2 Z 1–12: Studiengang und Studiengangsmanagement

Die nachfolgenden Kriterien sind unter Berücksichtigung einer heterogenen Studierendenschaft anzuwenden. Im Falle von Studiengängen mit besonderen Profilelementen ist zudem in den Darlegungen auf diese profilbestimmenden Besonderheiten einzugehen. Besondere Profilelemente sind z.B. verpflichtende berufspraktische Anteile im Falle von Masterstudiengängen, berufsbegleitende Organisationsformen, duale Studiengänge, Studiengänge mit Fernlehre, gemeinsame Studienprogramme bzw. gemeinsam eingerichtete Studien etc.

Studiengang und Studiengangsmanagement

1. Der Studiengang orientiert sich am Profil und an den Zielen der Fachhochschul-Einrichtung und steht in einem nachvollziehbaren Zusammenhang mit dem Entwicklungsplan

Der Studiengang „Cyber Security and Resilience“ stärkt das Profil der FH St. Pölten und trägt strategisch zur Erreichung der nationalen Themenführerschaft in Cyber- und IT-Sicherheit bei.

Somit orientiert sich der Studiengang an dem Profil und den Zielen der FH St. Pölten. Mit dem Studiengang wird konsequent die Strategie 2021 der FH St. Pölten in den Bereichen der Positionierung, der Weiterentwicklung, der Internationalisierung, der Interdisziplinarität sowie der thematischen Erweiterung umgesetzt. Ferner wird mit dem neuen Studiengang ein Beitrag zur digitalen Roadmap des Bundes und der Strategie Forschung, Technologie und Innovation (FTI) des Landes geleistet.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Studiengang und Studiengangsmanagement

2. Der Bedarf und die Akzeptanz für den Studiengang sind in Bezug auf klar definierte berufliche Tätigkeitsfelder nachvollziehbar dargestellt und in Bezug auf die geplante Zahl an Absolvent/inn/en bzw. Studienplätzen gegeben.

Der Bedarf wurde anhand umfassender Arbeitsmarkt-, Kohärenz- sowie Bedarfsanalysen ermittelt.

Das Ergebnis der Analysen unterstreicht die Notwendigkeit der Einführung des Studiengangs ausdrücklich. Im Antrag wird hierzu auf die Studie des ISC, einer internationalen Non-profit-Mitgliederorganisation für Cyber-Security-ExpertInnen, verwiesen, welche schätzt, dass der Cybersecurity-Personalstand in den Industrieländern global um 145% wachsen muss, um die Nachfragerlücke zu schließen. In der Kohärenzanalyse wird präzise die Abgrenzung des neuen Studiengangs zu den bestehenden erläutert. Ferner wird ausführlich auf das BewerberInnen-Potenzial eingegangen. Die Bedarfsanalyse untermauert erneut die Notwendigkeit der Einführung des neuen Studiengangs.

Die beruflichen Tätigkeitsfelder sowie die Qualifikationsprofile sind detailliert und nachvollziehbar, auch im Hinblick auf die geplante Zahl der Studienplätze, dargelegt.

Mitarbeiter in Leitungspositionen wie der Chief Information Security Officer (CISO) benötigen sowohl technische IT-Kompetenz als auch Managementkompetenz. Der neue Studiengang vermittelt beides. Ein weiteres Beispiel ist das Berufsbild des ICT Security Managers, der u.a. die Definition der IT-Sicherheitsrichtlinien und die Durchführung von IT-Risikoanalysen im Unternehmen verantwortet.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Studiengang und Studiengangsmanagement

3. Das Profil und die intendierten Lernergebnisse des Studiengangs sind klar formuliert, umfassen fachlich-wissenschaftliche, personale und soziale Kompetenzen und entsprechen den beruflichen Anforderungen sowie der jeweiligen Niveaustufe des Nationalen Qualifikationsrahmens. Im Falle reglementierter Berufe ist darzulegen, ob und unter welchen Voraussetzungen der Berufszugang gewährleistet ist.

Der Studiengang teilt sich in vier fachliche Kernbereiche:

- Organizational Cyber Security and Resilience,
- Technical Cyber Security and Resilience,
- Applied Security Competence und
- Advanced Cyber Security and Resilience

die je nach Spezialisierung eine organisatorische oder technische Vertiefung im Bereich Cybersecurity and Resilience darstellen. Der Aufbau des Curriculums sowie die zeitliche und inhaltliche Struktur der einzelnen Module in den vier Semestern sind klar dargelegt. Die Lernergebnisse, die in den einzelnen Modulen erworben werden, sind präzise beschrieben. Module wie das „Complex Problem Solving“ oder „Leadership“ stellen den Erwerb personaler, sozialer und Managementkompetenzen sicher. Die erworbenen Kompetenzen entsprechen den beruflichen Anforderungen für die im Antrag identifizierte Berufsfelder. Die Module des Curriculums spiegeln auch die Gewichtung zwischen dem Erwerb der technischen Kompetenz (70%) und der Managementkompetenz (30%), wie in der Diskussion mit der FH St. Pölten erläutert.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Studiengang und Studiengangsmanagement

4. Die Studiengangsbezeichnung und der akademische Grad, der von der AQ Austria gemäß § 6 Abs 2 FHStG festgelegt ist, entsprechen dem Profil des Studiengangs.

Die Studiengangsbezeichnung und der akademische Grad entsprechend dem Profil des Studiengangs.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Studiengang und Studiengangsmanagement

5. Inhalt und Aufbau des Studienplans gewährleisten das Erreichen der intendierten Lernergebnisse unter Verbindung von angewandter Forschung und Entwicklung und Lehre. Im Falle von Bachelor- und Diplomstudiengängen umfasst der Studienplan ein Berufspraktikum.

Die Struktur und der Aufbau des Studiengangs „Cyber-Security and Resilience“ gewährleisten das Erreichen der zu erwartenden Lernergebnisse.

Der Studiengang ist besonders geeignet für Studierende, die den Bachelor Informatik erworben haben. Für Studierende mit dem Bachelor IT-Security ist eher der bereits bestehende Masterstudiengang Information Security der FH. St. Pölten geeignet, da Lehrinhalte, die im Bachelor IT-Security vermittelt werden, teilweise auch im Master „Cyber-Security and Resilience“ wiederholt werden, wie im Gespräch mit der FH St. Pölten erläutert.

Die Module des Studiengangs adressieren alle Bereiche der Cybersicherheit, die von der Komponenten-, Netz-, System-, Software- bis zur Anwendungssicherheit reichen. Somit ist der Erwerb der notwendigen technischen Kompetenz gewährleistet. Der zeitliche Aufbau der Module ist nachvollziehbar und stellt sicher, dass die notwendigen Kompetenzen in einer sinnvollen zeitlichen und inhaltlichen Abhängigkeit erworben werden. Module wie z.B. „Leadership“ stellen sicher, dass die Sachkenntnis über den Betrieb und das Management von IT-Organisationen erworben wird.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Empfehlung:

Für einen Studiengang, der sowohl technische als auch Managementkompetenz vermittelt, ist die angemessene Breite und Tiefe der zu vermittelnden Inhalte essentiell. Das Gutachterteam empfiehlt daher regelmäßiges Feedback vom Firmenbeirat und anderen relevanten Stakeholdern einzuholen, um insbesondere die Tiefe der zu vermittelnden Inhalte ggfs. anzupassen.

Studiengang und Studiengangsmanagement

6. Die didaktische Konzeption der Module des Studiengangs gewährleistet das Erreichen der intendierten Lernergebnisse und fördert die aktive Beteiligung der Studierenden am Lernprozess..

Die didaktische Konzeption des Studiengangs ist auf die Aneignungsperspektive und Teilnehmerorientierung ausgerichtet. In den Lehrveranstaltungen werden unterschiedliche didaktische Formen, die von „Inverted Classroom“, Vorträgen, Diskussionen bis hin zu (Labor) Übungen reichen, angewandt. Somit ist gewährleistet, dass das Lernen aktiv, selbstgesteuert und konstruktiv erfolgt. Die Lernenden sind in einer aktiven Rolle und reflektieren selbstbestimmt über die zu lernenden Inhalte. Ferner unterstützt der geblockte Unterricht das "Accelerated Learning", um komplexe Inhalte in kurzer Zeit zu vermitteln und es den Studierenden zu ermöglichen, sich vertieft mit Lerninhalten befassen zu können. Der Blockunterricht beinhaltet eine dreitägige Präsenzphase. Die restlichen Tage werden für das Selbststudium aufgewendet. Dieser Ansatz unterstützt auch die individuelle Spezialisierung.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Studiengang und Studiengangsmanagement

7. Die mit den einzelnen Modulen verbundene Arbeitsbelastung ermöglicht das Erreichen der intendierten Lernergebnisse in der festgelegten Studiendauer, bei berufsbegleitenden Studiengängen unter Berücksichtigung der Berufstätigkeit. Das ECTS wird korrekt angewendet.

Jedes Modul ist mit ECTS-Punkten und entsprechender Stundenbelastung von 25 h pro ECTS Punkt versehen. Die Studierenden erwerben in den 4 Semestern des Studiums in jedem Semester 30 ECTS Punkte. Dies entspricht gängiger Praxis und einschlägigen Erfahrungen mit dem European Credit Transfer System. Damit ergibt sich für die Studierenden ein veranschlagter jährlicher Workload von 1.500 Arbeitsstunden. Das entspricht ebenfalls sowohl gängiger Praxis als auch den gesetzlichen Vorgaben des FHStG.

Nicht aufgeschlüsselt wurde das Verhältnis aus Präsenzveranstaltungen, Vor- und Nachbereitung dieser, E-Learning sowie Vorbereitung auf die Prüfungsleistung. Idealerweise wird eine solche Aufschlüsselung noch ergänzt, um die Module sowohl für Lehrende als auch Studierende transparenter zu gestalten.

Aus Sicht des Gutachterteams sind die angegebenen Lerninhalte mit den jeweiligen ECTS stimmig und die Planung ermöglicht die Absolvierung der Lehrveranstaltungen in der vorgesehenen Studiendauer. Da es sich beim Studium um ein Vollzeitstudium bzw. Duales Studium im zweiten und dritten Semester handelt, wurde eine mögliche Berufstätigkeit neben dem Studium nicht berücksichtigt. Im Rahmen der direkten Gespräche mittels Videokonferenz konnte vonseiten der Studierenden in Erfahrung gebracht werden, dass die Arbeitslast als herausfordernd aber angebracht empfunden wird.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Studiengang und Studiengangsmanagement

8. Eine Prüfungsordnung liegt vor. Die Prüfungsmethoden sind geeignet, um zu beurteilen, ob und inwieweit die intendierten Lernergebnisse erreicht wurden.

Die Prüfungsordnung für den Studiengang "Cyber-Security and Resilience" liegt vor. Die Prüfungsmethoden beinhalten mündliche Prüfungen, schriftliche Prüfungen bzw. Leistungsnachweise, praktisch-konstruktive Prüfungen bzw. Aufgaben sowie Projekte. Die einzelnen Prüfungsmethoden sind präzise in der Prüfungsordnung formuliert. Abweichende Prüfungsmethoden sind vorgesehen, falls die Ablegung von Prüfung in der vorgeschriebenen Methode z.B. durch Behinderung nicht möglich ist. Die Prüfungsmodalitäten wie z.B. die Festlegung der Prüfungstermine, die Einsicht in die Beurteilungsunterlagen, die Beurteilung von Leistungen, die Wiederholung von Prüfungen, die Beurteilung von Bachelor-, Diplom- und Masterarbeiten sind detailliert festgehalten. Wie erwartet wird die Handhabung von Plagiaten sowie die Ungültigerklärung von Prüfungen und wissenschaftlichen Arbeiten adressiert. Ferner wird auf Rechtsschutz, die Handhabung von Berufspraktika, das Auslandssemester sowie von Fotos, Film- und Tonaufnahmen eingegangen. Es wird festgestellt, dass die Prüfungsordnung alle erwarteten Inhalte zum Studienablauf, dem Prüfungsablauf, der Bewertung von Prüfungsleistungen und Prüfungsformen sowie -modalitäten enthält. Die Prüfungsmethoden sind für die Beurteilung der zu erreichenden Lernergebnisse geeignet und ausführlich beschrieben.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Studiengang und Studiengangsmanagement

9. Die Ausstellung eines Diploma Supplements, das den Vorgaben der Anlage 1 zu § 6 der Universitäts- und Hochschulstatistik- und Bildungsdokumentationsverordnung – UHSBV, StF: BGBl. II Nr. 216/2019 entspricht, ist vorgesehen⁶.

Die Ausstellung eines Diploma Supplements ist vorgesehen. Das Diploma Supplement entspricht den Vorgaben der Verordnung der Bundesministerin für Bildung, Wissenschaft und Forschung über die Übermittlung von Daten, die Führung von Evidenzen, die Codierung und die statistischen Auswertungen und Verarbeitungen von Universitäten, Pädagogischen Hochschulen, Erhalten von Fachhochschul-Studiengängen und Privatuniversitäten (Universitäts- und Hochschulstatistik- und Bildungsdokumentationsverordnung – UHSBV).

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Studiengang und Studiengangsmanagement

⁶ In der FH-Akkreditierungsverordnung 2019 wird noch auf die Anlage 2 das UniStEV 2004 verwiesen. Diese Verordnung wurde geändert und deshalb wurde der Text des Beurteilungskriteriums im Gutachten entsprechend angepasst.

10. Die Zugangsvoraussetzungen sind klar definiert, entsprechen hinsichtlich des Qualifikationsniveaus den im FHSStG vorgesehenen Regelungen und fördern die Durchlässigkeit des Bildungssystems.

Die fachlichen Zugangsvoraussetzungen sind ebenso simpel wie effektiv formuliert. Demnach erfüllen Studienbewerber*innen die fachlichen Qualifikationen, wenn ein abgeschlossener facheinschlägiger Fachhochschul-Bachelorstudiengang oder der Abschluss eines gleichwertigen Studiums an einer anerkannten inländischen oder ausländischen postsekundären Bildungseinrichtung vorliegt.

Schriftlich wurde ergänzt, dass facheinschlägige Studien jene sind, welche zumindest 60 ECTS im Bereich der Informatik, oder Fachwissen in folgenden Teilbereichen der Informatik haben: Betriebssystem, Software Engineering/Programmieren, Netzwerktechnik, Algorithmen & Datenstrukturen/Datenbanken.

Die Feststellung der Gleichwertigkeit obliegt dabei der Studiengangsleitung. Ermittelt diese, dass nur einzelne Ergänzungen auf die volle Gleichwertigkeit fehlen, so ist sie berechtigt, die Feststellung der Gleichwertigkeit mit der Auflage von Prüfungen zu verbinden, die während des Studiums abzulegen sind. Diese Form der Erhöhung der Durchlässigkeit wird vom Gutachterteam begrüßt.

Da es sich um einen englischsprachigen Studiengang handelt, ist des Weiteren ein Nachweis über entsprechende Sprachkenntnisse gefordert. Dieser kann entweder durch einen englischsprachigen Schul- oder Hochschulabschluss oder durch ein B2 – Zertifikat erbracht werden. Außerdem behält sich die Studiengangsleitung vor, bei Sprachkenntnisnachweisen, welche älter als vier Jahre sind, eine Einstufungs-/Feststellungsprüfung durchzuführen.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Studiengang und Studiengangsmanagement

11. Das Aufnahmeverfahren ist klar definiert, gewährleistet eine faire und transparente Auswahl der Bewerber/innen und entspricht den im FHSStG vorgesehenen Regelungen.

Aus dem Antrag geht klar definiert und transparent hervor, wie ein Aufnahmeverfahren ablaufen hat. Es gibt drei leistungsbezogene Kriterien für Aufnahmeverfahren, mit je eigener Gewichtung, welche wie folgt vorgelegt wurden:

- Ergebnis des computerbasierten Tests: 60%
- Englischsprachiges Aufnahmegespräch: 30%
- Durchschnittsnote des Zeugnisses: 10%

Schriftlich wurde dem Gutachterteam versichert, dass der ungewichtete Notenschnitt herangezogen wird, wodurch ein faires Aufnahmeverfahren auch mit Bewerber*innen ohne ECTS-Anrechnungspunkte im Zeugnis ermöglicht wird.

Die zur Reihung führende Bewertung wird von Aufnahmesenaten, bestehend aus Mitgliedern des Lehrkörpers des Studiengangs, überprüfbar und nachvollziehbar dokumentiert. Des Weiteren wird auf das Einheben von Gebühren oder Kautionen verzichtet. Damit entspricht das Aufnahmeverfahren den gesetzlichen Vorgaben.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Studiengang und Studiengangsmanagement

12. Verfahren zur Anerkennung von hochschulischen und außerhochschulischen Kompetenzen im Sinne der Anrechnung auf Prüfungen oder Teile des Studiums sind klar definiert, transparent und entsprechen den im FHStG vorgesehenen Regelungen. Bei der Anerkennung von hochschulischen Kompetenzen wird das Übereinkommen über die Anerkennung von Qualifikationen im Hochschulbereich in der europäischen Region (Lissabonner Anerkennungsübereinkommen) berücksichtigt.

Der Studiengang Cyber-Security and Resilience richtet sein Verfahren zur Anerkennung nachgewiesener Kenntnisse sehr nahe am FHStG aus. Anerkennungen werden lehrveranstaltungsbezogen durchgeführt, wobei die Studiengangsleitung die Gleichwertigkeit der nachgewiesenen Kenntnisse zur entsprechenden Lehrveranstaltung feststellt. Wissensüberprüfungen sind hierbei jedoch nicht kategorisch ausgeschlossen. Sollte die Feststellung der Gleichwertigkeit aufgrund fehlender oder nicht vollständig vorhandener Unterlagen von positiv absolvierten Prüfungen nicht möglich sein, so kann eine Wissensüberprüfung veranlasst werden.

Ebenfalls dem FHStG entsprechend, sichert der Studiengang zu, besondere Kenntnisse oder Erfahrungen aus der beruflichen Praxis in Bezug auf die Anerkennung von Lehrveranstaltungen oder des Berufspraktikums zu berücksichtigen. Auch wird die Anerkennung zwischen den Einrichtungen unterschiedlicher Länder im EHR, wie im Lissabonner Anerkennungsübereinkommen vorgesehen, ermöglicht.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

8.3 Beurteilungskriterium § 17 Abs 3 Z 1–7: Personal

Personal

1. Das Entwicklungsteam für den Studiengang ist in Hinblick auf das Profil des Studiengangs fach einschlägig wissenschaftlich bzw. berufspraktisch qualifiziert. Das Entwicklungsteam entspricht in der Zusammensetzung und hinsichtlich des Einsatzes in der Lehre den im FHStG festgelegten Voraussetzungen.

Im Entwicklungsteam sind sowohl hochkarätige wissenschaftliche Vertreter aus dem Umfeld der IT-Sicherheit als auch Mitglieder mit den für den Studiengang relevanten berufspraktischen Erfahrungen und Kompetenzen vertreten. Das Team setzt sich aus rund 17 internen Mitarbeitenden der FH St. Pölten und 13 externe Fachpersonen zusammen. Drei Personen verfügen über eine Habilitation oder gleichwertige Qualifikation im Fachbereich des Studiengangs, 25 Mitglieder über einen Nachweis der einschlägigen, aktuellen Praxiserfahrung in IT-Sicherheit. Ebenso vertreten sind die Leiterin des Service Hochschulentwicklung und der Leiter des Service and Competence Center for Innovation Teaching and Learning. Das Entwicklungsteam agierte autonom und unabhängig. Das Entwicklungsteam wurde nach den Bestimmungen des FHStG zusammengesetzt.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Personal

2. Die Fachhochschul-Einrichtung sieht für den Studiengang ausreichend Lehr- und Forschungspersonal und ausreichend nicht-wissenschaftliches Personal vor.

Für den Studiengang steht ausreichend Lehr- und Forschungspersonal sowie nicht-wissenschaftliches Personal zur Verfügung, wie aus den Unterlagen ersichtlich.

Im Antrag wird der Lehraufwand für 2020 bis 2025 ausgewiesen. Der Bedarf an haupt- und nebenberuflichem Lehrpersonal wird dargestellt. Im Vollausbau sind 13 hauptberufliche und 14 nebenberufliche Lehrende beteiligt und der Anteil der durch Nebenberufliche angebotenen Semesterwochenstunden (ASWS) beträgt 37%. Die Lehrveranstaltungen des ersten Studienjahrs, Personal und Lehrpensen sind im Antrag ausgewiesen. Ebenso liegen im Anhang die Lebensläufe dieser Lehrpersonen und für sämtliche Mitglieder des Entwicklungsteams bei. Für lehrendes Personal ist pro Vollzeit-Äquivalente (VZÄ) eine anteilige Jahresleistung von 28 ASWS vorgesehen. Dieses entspricht einer 50%-Auslastung. Die restlichen 50% sind für Forschung und administrative Tätigkeiten vorgesehen. Die Studiengangsleitung ist mit einer VZÄ im Vollausbau vorgesehen. Ferner ist eine direkte Studeingangsverwaltung mit 0,5 VZÄ vorgesehen.

Im Antrag wird die Betreuungsrelation für das erste und das zweite Studienjahr sowie die Betreuung der Masterarbeit dargelegt. Es wird jeweils der Anteil an hauptberuflichen Lehrenden im Vergleich zur Studierendenzahl ausgewiesen. Im ersten Studienjahr beträgt diese Relation 4,2, im zweiten 5,5 und bei der Masterarbeit 2,3.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Personal

3. Die Zusammensetzung des haupt- und nebenberuflichen Lehrkörpers gewährleistet eine angemessene Betreuung der Studierenden.

Der Lehrkörper besteht aus 13 haupt- und 14 nebenberuflichen Lehrpersonen. Der Anteil an durch nebenberufliche Dozierende angebotene Semesterwochenstunden beträgt 37%. Aus den im Anhang des Antrags enthaltenen Lebensläufen geht hervor, dass es im Lehrkörper eine ausgewogene Mischung an Dozierenden mit langjähriger, aktueller Praxiserfahrung und akademisch profilierten, international angesehenen Personen gibt. Das Lehrpersonal ist pädagogisch-didaktisch qualifiziert und wird durch Services für IT Infrastruktur und didaktische Fortbildung unterstützt.

Alle Lehrenden bieten den Studierenden, im Rahmen von Sprechstunden, fachspezifische oder wissenschaftliche Beratung, welche auch über die Lehre hinausgehen kann. Darüber hinaus bieten die Studiengänge im Stundenplan fest verankerte Sprechstunden der Studiengangsleitung.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Personal

4. Die fachlichen Kernbereiche des Studiengangs sind durch hauptberufliches wissenschaftlich qualifiziertes sowie durch berufspraktisch qualifiziertes Lehr- und Forschungspersonal abgedeckt.

Im Antrag werden die vier Kernbereiche Organizational Cyber Security and Resilience, Technical Cyber Security and Resilience, Applied Security Competence und Advanced Cyber Security and Resilience dargelegt. Für alle vier Kernbereiche werden die Lehrveranstaltungen und das geplante Personal aufgelistet. Die Lebensläufe dieser Lehrpersonen liegen dem Antrag bei und belegen die wissenschaftliche und berufspraktische Qualifikation für die entsprechenden Kernbereiche. Das für die Kernbereiche vorgesehene Personal ist mehrheitlich hauptberuflich an der FH St. Pölten angestellt. Pro Kernbereich sind rund ein bis zwei nebenberufliche Lehrende beteiligt.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Personal

5. Das Lehr- und Forschungspersonal ist den Anforderungen der im Studiengang vorgesehenen Tätigkeiten entsprechend wissenschaftlich, berufspraktisch und pädagogisch-didaktisch qualifiziert. Wenn für den Studiengang Fachhochschul-Professor/inn/en vorgesehen sind, orientiert sich die Fachhochschul-Einrichtung an den diesbezüglichen Anforderungen des UG. Für den Fall, dass eine Fachhochschul-Einrichtung nicht über eine ausreichende Anzahl an Fachhochschul-Professor/inn/en verfügt, um Auswahlkommissionen zu besetzen, ist bis zum Aufbau einer ausreichenden Kapazität an Professor/inn/en die Bestellung externer Professor/inn/en als Mitglieder der Auswahlkommission vorgesehen.

Das Lehr- und Forschungspersonal besteht im Vollausbau aus 29 Personen, wovon 13 hauptberufliche Lehrende sind. Das Lehr- und Forschungspersonal ist den Anforderungen der im Studiengang vorgesehenen Tätigkeiten entsprechend wissenschaftlich, berufspraktisch und pädagogisch-didaktisch qualifiziert, was u.a. durch die in den Unterlagen beigefügten wissenschaftlichen Publikationen belegt wird. Ferner ist die Zuordnung der Dozenten zu den Lehrveranstaltungen mit Angabe der ECTS-Kreditpunkte dargelegt.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Personal

6. Die Leitung für den Studiengang obliegt einer facheinschlägig wissenschaftlich qualifizierten Person, die diese Tätigkeit hauptberuflich ausübt.

Die Studiengangsleitung wird facheinschlägig und hauptberuflich eingesetzt. Wie aus den Unterlagen ersichtlich, wurde die Position gemäß den Anforderungen des FHStG öffentlich ausgeschrieben und soll baldmöglichst besetzt werden. Die Interims-Leitung hat der Leiter des Entwicklungsteams übernommen.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Personal

7. Die Gewichtung von Lehr-, Forschungs- und administrativen Tätigkeiten des hauptberuflichen Lehr- und Forschungspersonals gewährleistet sowohl eine angemessene Beteiligung an der Lehre in dem Studiengang als auch hinreichende zeitliche Freiräume für anwendungsbezogene Forschungs- und Entwicklungsarbeiten.

Die dem Antrag beiliegende Berechnung des Lehraufwands sieht für lehrendes Personal pro VZÄ eine anteilige Jahresleistung von 28 ASWS vor. Dies entspricht einer 50%-Auslastung. Die restlichen 50% sind für Forschung und administrative Tätigkeiten vorgesehen.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

8.4 Beurteilungskriterium § 17 Abs 4: Finanzierung

Finanzierung

Die Finanzierung des Studiengangs ist sichergestellt. Für die Finanzierung des Auslaufens des Studiengangs ist finanzielle Vorsorge getroffen.

Mit dem Antrag liegen ein Finanzierungsplan, ein Fördervertrag zwischen dem Land Niederösterreich und der FH St. Pölten sowie eine Nachreichung für die Präzisierung der ausgewiesenen IT- und Infrastrukturkosten vor.

Der vorliegende Finanzierungsplan zeigt die Finanzierung des Studiengangs für mindestens 5 Jahre, von Studienjahr 2020/21 bis und mit Studienjahr 2024/25. Wie im Antrag dargelegt, liegt dem Finanzierungsplan eine Kalkulation mit Ausweis der Kosten pro Studienplatz zugrunde.

Die Kalkulation basiert auf je 30 Studienplätzen pro Studienjahrgang. Das Studium dauert zwei Jahre. Im eingeschwungenen Zustand sind 60 Studienplätze pro Jahr finanziert. Die in der Finanzierung berücksichtigten angebotenen Semesterwochenstunden (ASWS) entsprechen den im Curriculum ausgewiesenen 54 ASWS für das erste Studienjahr und 41 ASWS für das zweite Studienjahr.

Kostenseitig werden Personal- und Betriebskosten berücksichtigt. Zudem werden Investitionen aufgeführt.

Die Personalkosten stehen in Bezug zum Personalbedarf. Die Kosten für das Lehr- und Forschungspersonal basieren auf dem im Antrag ausgeführten Personalbedarf sowie der je hälftigen Verteilung für haupt- und nebenberufliche Dozierende.

Die Betriebskosten werden in einer Nachreichung zum Antrag genauer erläutert. Insbesondere relevant für den vorliegenden Antrag sind IT-Kosten. Gemäß Nachreichung werden die Services für IT und Infrastruktur, Personal und Recht, Finanzen und Controlling sowie Bibliothek für die Fachhochschule St. Pölten GmbH unentgeltlich erbracht. Diese Services werden, gemäß Ausführung, durch die ehemalige Studienplatzförderung der Landeshauptstadt St. Pölten, seit 2018 als Gesellschafterzuschüsse finanziert. Die Gesellschafterinnen der FH St. Pölten GmbH sind 26% das Land Niederösterreich und 74% die die Hochschulen St. Pölten GmbH, deren Alleingeschafterin die Landeshauptstadt St. Pölten ist.

Die im Finanzierungsplan ausgewiesene Investition in EDV bezieht sich auf ein neues Cyber Defense Center, welches kontinuierlich angepasst und erneuert wird. In der Diskussion wurde erläutert, dass die Investitionen auf Departmentebene getätigt werden und sich die angegeben

Summen anteilmäßig auf den Studiengang beziehen. Die Gesamtinvestitionssumme für das Cyber Defense Center beläuft sich auf einen sechsstelligen Betrag.

Die Erträge weisen die Studienplatzförderung durch den Bund, Beiträge der Länder und Studiengebühren aus, wobei die Bundesförderung den eigentlichen Hauptanteil ausmacht. Für den Länderbeitrag liegt dem Antrag ein Fördervertrag zwischen dem Land Niederösterreich und der FH St. Pölten bei. Dieser belegt den Beitrag für den Zeitraum 2020 bis 2022. Eine Nachreichung zum Antrag erläutert zudem die kalkulatorischen Beiträge der Gemeinden. Es handle sich um kalkulatorische Umlagen, welche seit 2018 bei allen akkreditierten Studiengängen der FH St. Pölten so in dieser Form dargestellt werden.

Das Gutachterteam sieht den vorliegenden Finanzierungsplan als realistische Gegenüberstellung von Aufwand und Ertrag. Die Positionen sind transparent dargelegt und schlüssig.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

8.5 Beurteilungskriterium § 17 Abs 5: Infrastruktur

Infrastruktur

Für den Studiengang steht eine quantitativ und qualitativ adäquate Raum- und Sachausstattung zur Verfügung. Falls sich die Fachhochschul-Einrichtung externer Ressourcen bedient, ist ihre Verfügungsberechtigung hierüber vertraglich sichergestellt.

Während der Gespräche im Zuge des Akkreditierungsprozesses wurde dem Gutachterteam ein umfassendes Bild der Raum- und Laborausstattung, sowie der IT Infrastruktur vermittelt. Die Lehrräume entsprechen aktuellen Standards und Plätze sind auch lt. der Studierendenvertreter der bereits etablierten Studien, insb. des themenverwandten Studiums „IT Security“, immer in ausreichender Zahl vorhanden. Die Netzwerk- und Serverinfrastruktur (beispielsweise der Virtualisierungscluster) entspricht heutigen Maßstäben. Auch die in den einzelnen Lehrveranstaltungen planmäßig zum Einsatz kommenden Tools entsprechen den Erwartungen und durchaus den in der Wirtschaft nachgefragten Standards. Dies umfasst sowohl teure kommerzielle Speziallösungen als auch verstärkt für den professionellen Einsatz taugliche Open Source Lösungen. Viele Laborplätze werden bereits jetzt virtuell über einen eigenen VPN-Zugang angeboten; der Zugang soll 24/7 möglich sein.

Positiv fällt auch der Eindruck über das zu errichtende Cyber Defense Center (CDC) als Übungsumgebung für Studierende aus, welches im Zuge dieses Studiums zum Einsatz kommen soll.

Das Gutachterteam kommt daher zum Schluss, dass dieses Kriterium als **erfüllt** zu bewerten ist.

8.6 Beurteilungskriterium § 17 Abs 6 Z 1–2: Angewandte Forschung und Entwicklung

Angewandte Forschung und Entwicklung

1. Das dem Studiengang zugeordnete hauptberufliche Lehr- und Forschungspersonal ist in für den Studiengang fachlich relevante anwendungsbezogene Forschungs- und Entwicklungsarbeiten der Fachhochschul-Einrichtung eingebunden.

Die Verankerung der angewandten Forschung und Entwicklung in der akademischen Aus- und Weiterbildung ist ein wesentlicher Eckpfeiler der Strategie der FH St. Pölten. Für hauptberuflich Lehrende gehört Forschung und Entwicklung zu den zentralen Aufgaben laut Anforderungsprofil. Sie sind nachweislich in (nationalen) Forschungsprojekten tätig. Die Integration der angewandten Forschung in den Lehrbetrieb ist durch das Abhalten von Lehrveranstaltungen durch Forschungspersonal gegeben. Zudem ist für hauptberuflich Lehrende eine Reduktion der Lehrverpflichtung im Hinblick auf ihre Forschungstätigkeit vorgesehen.

Forschungs- und Entwicklungsarbeiten des hauptberuflichen Lehr- und Forschungspersonals des Studienganges sind vielfältig und umfassen neben der eigentlichen Forschungsarbeit im Zuge von Forschungsprojekten, auch die Publikation in einschlägigen Journalen und Fachzeitschriften, genauso wie die Präsentation von Ergebnissen auf Konferenzen, sowie die Teilnahme (und auch Abhaltung) von Security-spezifischen Veranstaltungen. Letztere sind auch wesentlich für den Wissenstransfer, wobei insb. die Organisation der in Österreich sehr bekannten und jährlich stattfindenden ITSecX Veranstaltung (IT Security Community XChange) Beleg für die erfolgreiche Abhaltung von facheinschlägigen Veranstaltungen ist. Auch die Etablierung mehrerer Kompetenzzentren durch und unter Mitwirkung von hauptberuflichem Lehr- und Forschungspersonal im Bereich der Security, wie beispielsweise dem Josef Ressel-Zentrum für Blockchain-Technologien & Sicherheitsmanagement, als auch dem Josef Ressel-Zentrum für konsolidierte Erkennung von gezielten Angriffen, sind Belege für die forschungsorientierte Gestaltung des IT-Security Bereichs.

Die Einbindung von Studierenden in die Forschungs- und Entwicklungstätigkeiten des Studiengangs ist durch die Möglichkeit gegeben ihre Masterarbeit im Rahmen eines F&E-Projektes an der Fachhochschule oder bei einem/einer IndustriepartnerIn durchzuführen. Interdisziplinarität aufgrund der existierenden Forschungsschwerpunkte der Fakultät ist in hohem Maße gegeben.

Das Gutachterteam kommt somit zum Schluss, dass das dem Studiengang zugeordnete hauptberufliche Lehr- und Forschungspersonal in für den Studiengang fachlich relevante anwendungsbezogene Forschungs- und Entwicklungsarbeiten der Fachhochschul-Einrichtung hinreichend eingebunden ist.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

Angewandte Forschung und Entwicklung

2. Die (geplanten) Forschungsleistungen des dem Studiengang zugeordneten hauptberuflichen Lehr- und Forschungspersonals entsprechen dem hochschulischen Anspruch und der jeweiligen Fächerkultur.

In ihrer Strategie strebt die FH St. Pölten eine ganzheitlich qualitätsvolle Weiterentwicklung in ihren drei Leistungsbereichen (1) Akademische Aus- und Weiterbildung, (2) Angewandte Forschung und Entwicklung, sowie (3) Wissenstransfer und Innovation an. Die enge Vernetzung und Verzahnung dieser drei Bereiche ist essentieller Teil der Strategie der FH St. Pölten. Sie erhebt den Anspruch messbare hohe Forschungsleistungen zu erbringen, die intensive Vernetzung mit der wissenschaftlichen Community zu gewährleisten, nennenswerte Beiträge zu

regionalen und nationalen Innovationssystemen zu liefern und eine sehr gute öffentliche Wahrnehmung im nationalen Umfeld zu erreichen.

Die Qualität der Forschungsleistungen lässt sich überwiegend durch einschlägige Publikationen beurteilen. Das an der FH St. Pölten am Institut für IT-Sicherheitsforschung tätige hauptberufliche Lehr- und Forschungspersonal bringt nachweislich regelmäßig Publikationen hervor und präsentiert diese auch auf wissenschaftlichen Konferenzen. In den letzten Jahren finden sich in der Liste der Veröffentlichungen durchaus auch hochkarätige Konferenzen und Fachzeitschriften, wie z.B. die IFIP Sec oder ARES Konferenz, sowie das Elsevier Journal of Computers & Security.

Neben den Publikationsleistungen ist jedoch auch die erfolgreiche Einwerbung von einschlägigen Forschungsprojekten, die meist neben der Sicherstellung der Finanzierung v.a. den für die Forschung wesentlichen Kooperationsrahmen mit Partnerinstituten eröffnen, wichtiger Bestandteil für die Erbringung hoher Forschungsleistungen. Dabei ist die FH St. Pölten ebenfalls erfolgreich. Dies ist vor allem durch eine Vielzahl an fach-relevanten, von der österreichischen Forschungsförderungsgesellschaft FFG geförderten Forschungsprojekten in den Sicherheitsforschungsprogrammen KIRAS und FORTE belegt. In diesen Projekten hat das hauptberufliche Lehr- und Forschungspersonal der FH oft auch führende Rollen inne. Eine Vielzahl für eine Bildungsinstitution sinnvolle Initiativen, wie beispielsweise FFG Qualifizierungsnetze und FFG Digital Pro Bootcamps, runden dieses Profil ab. Im Hinblick auf eine weitere Stärkung des wissenschaftlichen Profils und Erweiterung der Kooperationsmöglichkeiten wäre mittelfristig eine Teilnahme an internationalen Forschungsprojekten, z.B. in den Rahmenprogrammen der EU, eine attraktive Entwicklungsmöglichkeit.

Die Forschungsleistungen des dem Studiengang zugeordneten hauptberuflichen Lehr- und Forschungspersonals entsprechen aufgrund der o.g. Gründe dem hochschulischen Anspruch und der jeweiligen Fächerkultur.

Das Kriterium wird seitens des Gutachterteams als **erfüllt** eingestuft.

8.7 Beurteilungskriterium § 17 Abs 7: Kooperationen

Kooperationen

Für den Studiengang sieht die Fachhochschul-Einrichtung entsprechend seinem Profil Kooperationen mit hochschulischen und gegebenenfalls nicht-hochschulischen Partner/inne/n im In- und Ausland vor, die auch die Mobilität von Studierenden und Personal fördern.

Die angestrebten bzw. mit dem Institut für IT Sicherheitsforschung bereits etablierten Kooperationen entsprechen dem Studiengangsprofil. Besonders hervorzuheben sind die Kooperationen mit namhaften österreichischen Unternehmen, darunter Frequentis AG, Ikarus Software GmbH, SEC-Consult und T-Systems Austria. Viele dieser Unternehmen sind international tätig und erstklassig vernetzt. Internationale Großunternehmen, wie beispielsweise Airbus oder die KPMG runden dieses Unternehmensnetzwerk ab. Im Zuge der Kooperationen ist einerseits geplant, Gastvorträge zu organisieren und so den Studierenden die Security-Herausforderungen in der Wirtschaft aus erster Hand zu vermitteln, andererseits sind alle angeführten Partner auch duale Ausbildungspartner für Studierende des Studiengangs.

Weiters kann die FH St. Pölten für den gegenständlichen Studiengang auch Kooperationen mit akademischen Partnern nachweisen. Gastvorträge und gemeinsame Forschungsvorhaben sind mit der Universität Wien und der Technischen Universität Graz geplant. Internationale Partnerinstitutionen sind beispielsweise die Pennsylvania State University, mit der gemeinsam

auch die Summer School ICCSA abgehalten wird, die Sungkyunkwan University, Seoul Women University und University of New South Wales. Mit all diesen Institutionen bestehen Kooperationsabkommen in den unterschiedlichen, für den gegenständlichen Studiengang relevanten, Fachbereichen.

Das Netzwerk der FH St. Pölten könnte durch eine weitere Öffnung und Anschluss an die europäische Hochschullandschaft auch im Hinblick auf gemeinsame Forschungsprojekte im europäischen Kontext deutlich profitieren.

Die FH St. Pölten ist Mitglied in mehreren Gremien und Interessensverbänden. Hier wäre beispielsweise das „Citizen Science Network Austria“ zu nennen, aber auch Mitgliedschaften in zahlreichen Netzwerken und Plattformen sowohl im Umfeld ihrer fachlich-inhaltlichen Schwerpunkte als auch im bildungs-, forschungs- und hochschulpolitischen Umfeld (z.B. EAIE – European Association for International Education, UIIN - University Industry Innovation Network, EUA - European University Association). Daneben findet der individuelle Austausch von Angehörigen der FH St. Pölten auf (inter-)nationaler inter-institutioneller Ebene im Zuge einschlägiger Veranstaltungen statt.

Die Mobilität von Studierenden und Lehrenden wird ermöglicht und aktiv gefördert. Das sog. Mobilitätsfenster soll es Studierenden ermöglichen auch mehrere Semester im Ausland zu verbringen, wobei sich dafür insbesondere das vierte Semester anbietet, welches zur Erstellung der Masterarbeit vorgesehen ist. Positiv hervorzuheben ist, dass abseits der „klassischen“ Auslandssemester auch weitere Maßnahmen zur Mobilität im Studiengang etabliert werden sollen bzw. durch die Institution bereits etabliert sind. Im Rahmen von Kurzaufenthalten, wie beispielsweise Summer Schools, ist es den Studierenden möglich, einen Auslandsaufenthalt auf einer anderen Hochschule zu absolvieren. Auf dem Gebiet der Informationssicherheit besteht hier seit mehreren Jahren eine sehr erfolgreiche Kooperation (ICSSA Summer School) mit der Pennsylvania State University, Sungkyunkwan University und Seoul Women University.

Es wird aus Sicht des Gutachterteams festgehalten, dass das Kriterium als **erfüllt** bewertet wird.

9 Zusammenfassung und abschließende Bewertung

Entwicklung und Qualitätssicherung des Studiengangs:

Der Studiengang wurde anhand eines definierten Prozesses zur Entwicklung und Einrichtung von Studiengängen entwickelt. Dabei wurde gewährleistet, dass alle relevanten Stakeholder aktiv an der Entwicklung des Studiengangs beteiligt sind. Der Studiengang ist nach erfolgreicher Akkreditierung in das Qualitätsmanagement der Fachschule eingebunden, welches alle Leistungsbereiche der Hochschule umfasst und regelmäßig evaluiert wird.

Studiengang und Studiengangsmanagement:

Mit dem geplanten Masterstudiengang „Cyber-Security and Resilience“ ergänzt die FH St. Pölten ihr bisheriges Portfolio an Studiengängen in sinnvoller Weise, orientiert sich dabei an ihren Zielsetzungen und steht in einem nachvollziehbaren Zusammenhang mit deren Entwicklungsplan. Die 30 Studienanfängerplätze sind bereits zum Zeitpunkt der Videokonferenz des Gutachterteams mit der FH St. Pölten gut nachgefragt.

Personal:

Für den Studiengang steht ausreichend Lehr- und Forschungspersonal sowie nicht-wissenschaftliches Personal zur Verfügung. Das Personal ist wissenschaftlich, berufspraktisch und pädagogisch-didaktisch qualifiziert. Die Studiengangsleitung wird facheinschlägig und

hauptberuflich eingesetzt. Im Entwicklungsteam sind hochkarätige wissenschaftliche Vertreter und Personen mit einschlägigen, berufspraktischen Kompetenzen vertreten. Die Betreuung der Studierenden durch haupt- und nebenberufliche Lehrenden ist gewährleistet und die Beteiligung des hauptberuflichen Personals an Lehre, Forschungs- sowie Entwicklungsarbeiten ist angemessen.

Finanzierung:

Die Finanzierung des Studiengangs ist sichergestellt. Der vorliegende Finanzierungsplan zeigt eine realistische Gegenüberstellung von Aufwand und Ertrag und nachhaltige Finanzierung entsprechend dem Entwicklungsplans des Studiengangs.

Infrastruktur:

Die Netzwerk- und Serverinfrastruktur entspricht heutigen Maßstäben, die Raum- und Platzsituation erlaubt die effektive Abhaltung der geplanten Lehrveranstaltungen. Viele Laborplätze werden bereits jetzt virtuell über einen eigenen VPN-Zugang angeboten.

Angewandte Forschung und Entwicklung:

Die Verankerung der angewandten Forschung und Entwicklung in der akademischen Aus- und Weiterbildung ist ein wesentlicher Eckpfeiler der Strategie der FH St. Pölten. Die Einbindung von Studierenden in die Forschungs- und Entwicklungstätigkeiten des Studiengangs ist durch die Möglichkeit gegeben ihre Masterarbeit im Rahmen eines F&E-Projektes an der Fachhochschule oder bei einem/einer IndustriepartnerIn durchzuführen.

Kooperationen:

Die Zusammenarbeit mit namhaften österreichischen Unternehmen, darunter vielen international tätigen Partnern, sowie die Vernetzung der FH St. Pölten im akademischen Bereich, stellen sehr gute Bedingungen für Studierende dar, Einblicke in die Security Community durch Gastvorträge, Praktika und Projektarbeiten mit fach einschlägigen Stakeholdern zu gewinnen. Insbesondere werden dadurch Studierenden Security-Herausforderungen in der Wirtschaft aus erster Hand vermittelt.

Das Gutachterteam empfiehlt dem Board der AQ Austria die Akkreditierung des Masterstudiengangs „Cyber-Security and Resilience“.

Das Gutachterteam empfiehlt dem Board der AQ Austria die Akkreditierung des Masterstudiengangs „Cyber-Security and Resilience“.

10 Eingesehene Dokumente

- Antrag auf Akkreditierung des Masterstudiengangs „Cyber-Security and Resilience“, der Fachhochschule St.Pölten, durchgeführt in St.Pölten, vom 19.12.2019 in der Version vom 26.02.2020
- Nachreichungen vor dem Vor-Ort-Besuch:
 - Schriftliche Antwort auf die Fragen des Gutachterteams (11.05)
 - eine um ein Abbildungsverzeichnis ergänzte Version des Antrags (11.05)
 - Erklärung der FH St.Pölten zum Nachweis der Gemeindeförderung (11.05.2020)
 - Nachweis über die Förderung des Studiengangs durch das Bundesland Niederösterreich (11.05.2020)



AQ Austria, 1190 Wien, Franz-Klein-Gasse 5

- Nachreichungen nach dem Vor-Ort-Besuch:
 - Darstellung des internen Genehmigungsprozesses bei der Einrichtung eines Studiengangs sowie der Einbeziehung der studentischen Perspektive in diesen Prozess (19.05.2020)

Stellungnahme zum Gutachten im Rahmen des Akkreditierungsverfahrens zum FH-Masterstudiengang Cyber Security and Resilience – Stkz 0863

Sehr geehrte Frau Präsidentin Prof. Dr. Hanft,
sehr geehrte Mitglieder des Boards,
sehr geehrte Damen und Herren,

wir bedanken uns für die Übermittlung des ausführlichen Berichts der GutachterInnen und freuen uns über die durchwegs positive Bewertung des Akkreditierungsantrags betreffend die Akkreditierung des FH-Masterstudiengangs Cyber Security and Resilience.

Zu den aus unserer Sicht wesentlichsten Empfehlungen der GutachterInnen nehmen wir wie folgt Stellung:

- Das GutachterInnenteam empfiehlt die Stärken des neuen Studiengangs konsequent hervorzuheben, den Studierenden sowohl fundiertes IT-Sicherheitswissen zu vermitteln als auch diese auf die zukünftigen Managementaufgaben vorzubereiten.

Für die Bewerbung und Umsetzung des Studienprogramms greifen wir daher die, von den GutachterInnen empfohlenen Maßnahmen gerne auf:

Die Bewerbung des Studiengangs erfolgt auf unterschiedlichen, gängigen Kanälen (Webseite, Social Media, Folder, Bildungsmessen etc.), in den Texten werden in Zukunft die Stärken des Studiengangs noch deutlicher hervorgehoben. Auch in den Gesprächen mit potenziellen Studierenden wird diese Empfehlung des GutachterInnen-Teams Berücksichtigung finden.

- Im Gutachten wird angemerkt, dass für einen Studiengang, der sowohl technische als auch Managementkompetenz vermittelt, die angemessene Breite und Tiefe der zu vermittelnden Inhalte essentiell ist. Das GutachterInnen-Team empfiehlt daher regelmäßiges Feedback vom Firmenbeirat und anderen relevanten Stakeholdern einzuholen, um insbesondere die Tiefe der zu vermittelnden Inhalte ggf. anzupassen.

Für die Umsetzung des Studienprogramms halten wir folgendes fest:

Alle Studiengänge der FH St. Pölten werden einer regelmäßigen Evaluierung unterzogen, dabei werden alle relevanten Stakeholder zum Studiengang befragt. Spätestens im Rahmen

dieser Überprüfung und der sich daraus ergebenden Änderungen, soll diese Empfehlung des GutachterInnen-Teams Eingang in die Qualitätssicherung des Studiengangs finden.

- Im Gutachten wird angemerkt, dass im Antrag auf Akkreditierung das Verhältnis aus Präsenzveranstaltungen, Vor- und Nachbereitung dieser, E-Learning sowie die Vorbereitung auf die Prüfungsleistung nicht explizit aufgeschlüsselt wurde und eine solche Ergänzung sowohl für Lehrende als auch für Studierende mehr Transparenz gewährleisten würde.

Für die Umsetzung des Studiengangs halten wir an dieser Stelle folgendes fest:

In der Vorbereitung der jeweiligen Semester werden diese Daten in Abstimmung mit den Lehrenden aufgeschlüsselt und den Studierenden rechtzeitig und auf entsprechende Weise zur Kenntnis gebracht.

Abschließend möchten wir uns bei den GutachterInnen für das Gutachten, die wertvollen Hinweise und die konstruktiven und wertschätzenden Gespräche im Zuge des virtuellen GutachterInnen-Gesprächs bedanken. Unser Dank gilt auch der AQ Austria für die kompetente und flexible Verfahrensbegleitung, trotz der durch die Covid-19 verursachten Umstände.

Mit freundlichen Grüßen

St. Pölten, am 25.06.2020