

Fachspezifische Studien- und Prüfungsordnung für den Masterstudiengang Cybersecurity an der Universität Potsdam

Vom XXXX

Der Fakultätsrat der Digital Engineering Fakultät der Universität Potsdam hat auf der Grundlage der §§ 19 Abs. 1, 22 Abs. 1-3, 31 i. V. m. § 72 Abs. 2 Nr. 1 des Brandenburgischen Hochschulgesetzes (BbgHG) vom 28. April 2014 (GVBl.I/14, [Nr. 18]), zuletzt geändert durch Artikel 2 des Gesetzes vom 20. September 2018 (GVBl.I/18, [Nr. 21], S. 2) in Verbindung mit der Verordnung über die Gestaltung von Prüfungsordnungen zur Gewährleistung der Gleichwertigkeit von Studium, Prüfungen und Abschlüssen (Hochschulprüfungsverordnung - HSPV) vom 4. März 2015 (GVBl.II/15, [Nr. 12]) und mit Art. 21 Abs. 2 Nr. 1 der Grundordnung der Universität Potsdam (GrundO) vom 17. Dezember 2009 (AmBek. UP Nr. 4/2010 S. 60) in der Fassung der Fünften Satzung zur Änderung der Grundordnung der Universität Potsdam (GrundO) vom 24. August 2018 (AmBek. UP Nr. 11/2018 S. 634) und § 1 Abs. 2 der Neufassung der allgemeinen Studien- und Prüfungsordnung für die nicht lehramtsbezogenen Bachelor- und Masterstudiengänge an der Universität Potsdam vom 30. Januar 2013 (BAMA-O) (AmBek UP Nr. 3/2013, S. 35), zuletzt geändert am 18. April 2018 (AmBek UP Nr. 6/2018, S. 370), am XXXX folgende Studien- und Prüfungsordnung als Satzung beschlossen:¹

Inhalt

| | |
|-----|--|
| § 1 | Geltungsbereich |
| § 2 | Abschlussgrade |
| § 3 | Ziel des Studiums und Berufsrelevanz |
| § 4 | Dauer und Gliederung des Studiums |
| § 5 | Studienreferat; Leistungserfassungsprozess |
| § 6 | Module des Masterstudiums |
| § 7 | Masterarbeit |
| § 8 | Freiversuche |
| § 9 | In-Kraft-Treten |

Anlagen

| | |
|----------|--|
| Anlage 1 | Modulkatalog |
| Anlage 2 | Exemplarische Studienverlaufspläne für das Masterstudium |

§ 1 Geltungsbereich

(1) Diese Ordnung gilt für das Masterstudium im Fach *Cybersecurity* an der Digital Engineering Fakultät der Universität Potsdam. Sie ergänzt als fachspezifische Ordnung die Neufassung der allgemeinen Studien- und Prüfungsordnung für die nichtlehramtsbezogenen Bachelor- und Masterstudiengänge an der Universität Potsdam (BAMA-O).

(2) Bei Widersprüchen zwischen dieser Ordnung und der BAMA-O gehen die Bestimmungen der BAMA-O den Bestimmungen dieser Ordnung vor.

§ 2 Abschlussgrad

Nach Erwerb der erforderlichen Leistungspunkte und nach Vorlage der Graduierungsvoraussetzungen verleiht die Universität Potsdam durch die Digital Engineering Fakultät den akademischen Grad eines „Master of Science“, abgekürzt „M.Sc.“.

§ 3 Ziel des Studiums und Berufsrelevanz

(1) Das konsekutive Masterstudium ist ein wissenschafts- und forschungsorientiertes Studium, das vertiefte wissenschaftliche Grundlagen, erweiterte Fachkenntnisse und Fähigkeiten im Bereich Cybersecurity sowie spezialisierte Methoden-, Sozial- und Selbstkompetenzen vermittelt.

(2) Absolventinnen und Absolventen des Masterstudiums verfügen über ein breites Spektrum an Fähigkeiten und Kenntnissen zu Theorien, Konzepten, Methoden, Techniken und Verfahren skalierbarer Sicherheitssysteme sowie der damit verbundenen Management- und Leitungsaufgaben. Zusätzlich erlangen sie vertiefte fachwissenschaftliche Kenntnisse in den gewählten Vertiefungsgebieten aus dem Bereich Cybersecurity. Sie sind in der Lage, verantwortlich in Teams zu wirken sowie arbeitsteilig zu planen, durchzuführen, zu bewerten, zu steuern und die erarbeiteten Ergebnisse verständlich zu kommunizieren. Sie können zu ethischen und rechtlichen Fragen geeignete Lösungskonzepte und -strategien auswählen und anwenden. Darüber hinaus sind sie geschult im Umgang mit vertraulichen Sicherheitsdaten, der Wahrung von Privatsphäre und der Anwendung geeigneter Methoden zum Schutz personenbezogener und personenbeziehbarer Daten. Sie verfügen über ausgeprägte Fähigkeiten fremdsprachlicher Fachkommunikation in Englisch.

¹ Genehmigt durch den Präsidenten der Universität Potsdam am XX. XX. 2018.

(3) Das Masterstudium vermittelt Studierenden zudem vertiefte Kenntnisse und Fähigkeiten, die zur wissenschaftlichen Arbeit, zur wissenschaftlich fundierten Urteilsbildung, zur kritischen Reflexion fachbezogener Erkenntnisse und zum verantwortlichen Handeln notwendig sind; weitergehende Schlüsselfertigkeiten werden dazu in den Bereichen Methodenkompetenz, Sozialkompetenz und Selbstkompetenz vermittelt. Insbesondere erlangen die Absolventinnen und Absolventen Schlüsselfertigkeiten, die vor allem für die Konzeption, Implementierung und Erforschung skalierbarer Sicherheitssysteme sowie für die damit verbundene Beurteilung ethischer und rechtlicher Fragestellungen benötigt werden.

(4) Die Absolventinnen und Absolventen des Masterstudiengangs erhalten einen weiteren berufsqualifizierenden Abschluss. Sie sind in der Lage Leitungs- und Führungspositionen insbesondere dort einzunehmen, wo der Entwurf, die Realisierung, die Wartung und der Betrieb komplexer Sicherheitssysteme eine wesentliche Rolle spielen (z. B. als Cybersecurity Engineer, IT Security Engineer, Cybersecurity Analyst, IT-Unternehmerin und IT-Unternehmer u.a.). Sie sind ferner in der Lage, Entwicklungs- und Forschungsarbeiten eigenständig durchzuführen, Unternehmen mit IT-Schwerpunkt aufzubauen oder sich in einem nachfolgenden Promotionsstudium wissenschaftlich weiter zu qualifizieren.

§ 4 Dauer und Gliederung des Studiums

(1) Das Masterstudium im Fach *Cybersecurity* wird an der Universität Potsdam als Ein-Fach-Studium mit 120 Leistungspunkten angeboten. Die Regelstudienzeit des Masterstudiums beträgt vier Semester.

(2) Das Masterstudium gliedert sich wie folgt:

| | |
|--|---------------|
| Pflichtmodule | 48 LP |
| Wahlpflichtmodule (Vertiefungsgebiete) | 36 LP |
| Wahlpflichtmodule (Soft Skills) | 6 LP |
| Masterarbeit | 30 LP |
| Insgesamt | 120 LP |

§ 5 Studienreferat; Leistungserfassungsprozess

Für diesen Studiengang ist an der Digital Engineering Fakultät ein Studienreferat eingerichtet, welches die in der BAMA-O dem Studienbüro zugewiesenen Aufgaben wahrnimmt.

§ 6 Module des Masterstudiums

(1) Das Masterstudium im Studiengang *Cybersecurity* setzt sich aus folgenden Bestandteilen zusammen:

| <i>Kennung</i> | <i>Titel</i> | <i>LP</i> |
|---|--------------------------------|-----------|
| I Pflichtmodule (48 LP) | | |
| CS: Cybersecurity | | |
| HPI-CS-T | Security Technologies | 6 |
| HPI-CS-C | Advanced Cryptography | 6 |
| HPI-CS-S | Systems and Network Security | 6 |
| HPI-CS-A | Application Security | 6 |
| HPI-CS-PE | Data Protection & Ethics | 6 |
| HPI-DE-RWM | Recht, Wirtschaft, Management | 6 |
| HPI-CS-L | Security Lab | 12 |
| II Wahlpflichtmodule | | |
| <i>Vertiefungsgebiete (36 LP)</i> | | |
| <i>Es sind insgesamt zwei Vertiefungsgebiete zu absolvieren (3 x 6 LP bestehend aus Konzepten und Methoden (K), Techniken und Werkzeuge (T) und Spezialisierung (S)).</i> | | |
| SECA: Security Analytics | | |
| HPI-SECA-K | SECA – Konzepte und Methoden | 6 |
| HPI-SECA-T | SECA – Techniken und Werkzeuge | 6 |
| HPI-SECA-S | SECA – Spezialisierung | 6 |
| IDMG: Identity Management | | |
| HPI-IDMG-K | IDMG – Konzepte und Methoden | 6 |
| HPI-IDMG-T | IDMG – Techniken und Werkzeuge | 6 |
| HPI-IDMG-S | IDMG – Spezialisierung | 6 |
| CYAD: Cyber Attack and Defense | | |
| HPI-CYAD-K | CYAD – Konzepte und Methoden | 6 |
| HPI-CYAD-T | CYAD – Techniken und Werkzeuge | 6 |
| HPI-CYAD-S | CYAD – Spezialisierung | 6 |
| <i>Weitere Wahlpflichtmodule (6 LP)</i> | | |
| <i>Es ist ein Modul aus SSK zu wählen.</i> | | |
| HPI-SSK-KO | Kommunikation | 6 |
| HPI-SSK-ML | Management und Leitung | 6 |
| HPI-SSKDTB | Design Thinking Basics | 6 |
| HPI-SSKDTA | Design Thinking Advanced | 6 |
| III Masterarbeit | | 30 |

(2) Die Lehrsprache im Masterstudiengang *Cybersecurity* ist Deutsch.

(3) Näheres zu den in Abs. 1 genannten Modulen regelt Anhang 1: Modulkatalog zu dieser Satzung.

(4) Ein exemplarischer Studienverlaufsplan ist in Anlage 2 zu dieser Ordnung aufgeführt.

§ 7 Masterarbeit

(1) Sobald die bzw. der Studierende 72 Leistungspunkte erworben hat, hat die bzw. der Studierende Anspruch auf die unverzügliche Vergabe eines Themas für die Masterarbeit.

(2) Diese Masterarbeit hat inklusive der Disputation einen Umfang von 30 Leistungspunkten.

§ 8 Freiversuche

Im Masterstudium *Cybersecurity* können zwei Freiversuche mit Ausnahme des Moduls Security Lab in Anspruch genommen werden.

§ 9 In-Kraft-Treten

(1) Diese Ordnung tritt am Tage nach der Veröffentlichung in den Amtlichen Bekanntmachungen der Universität Potsdam in Kraft.

(2) Diese Ordnung gilt für alle Studierenden, die nach dem In-Kraft-Treten dieser Ordnung an der Universität Potsdam im Masterstudiengang *Cybersecurity* immatrikuliert werden.

Anlage 1: Modulkatalog

Die Beschreibungen der in § 6 Abs. 1 sowie in den folgenden Tabellen aufgeführten Module des Studiengangs regelt die Satzung für den Modulkatalog der Digital Engineering Fakultät für Bachelor- und Masterstudiengänge an der Universität Potsdam (MK DEF). Ergänzende Regelungen bzw. Abweichungen von den Regelungen des MK DEF sind den folgenden Tabellen zu entnehmen.

| Modul-Nr. | Modultitel | LP | PM/ WPM | Zugangsvoraussetzung |
|------------|--|----|------------|----------------------|
| HPI-CS-T | Security Technologies | 6 | PM | Siehe MK DEF |
| HPI-CS-C | Advanced Cryptography | 6 | PM | Siehe MK DEF |
| HPI-CS-S | Systems and Network Security | 6 | PM | Siehe MK DEF |
| HPI-CS-A | Application Security | 6 | PM | Siehe MK DEF |
| HPI-CS-PE | Data Protection & Ethics | 6 | PM | Siehe MK DEF |
| HPI-DE-RWM | Recht, Wirtschaft, Management | 6 | PM | Siehe MK DEF |
| HPI-CS-L | Security Lab | 12 | PM | Siehe MK DEF |
| HPI-SECA-K | Security Analytics – Konzepte und Methoden | 6 | WPM | Siehe MK DEF |
| HPI-SECA-T | Security Analytics – Techniken und Werkzeuge | 6 | WPM | Siehe MK DEF |
| HPI-SECA-S | Security Analytics – Spezialisierung | 6 | WPM | Siehe MK DEF |
| HPI-IDMG-K | Identity Management – Konzepte und Methoden | 6 | WPM | Siehe MK DEF |
| HPI-IDMG-T | Identity Management – Techniken und Werkzeuge | 6 | WPM | Siehe MK DEF |
| HPI-IDMG-S | Identity Management – Spezialisierung | 6 | WPM | Siehe MK DEF |
| HPI-CYAD-K | Cyber Attack and Defense – Konzepte und Methoden | 6 | WPM | Siehe MK DEF |
| HPI-CYAD-T | Cyber Attack and Defense – Techniken und Werkzeuge | 6 | WPM | Siehe MK DEF |
| HPI-CYAD-S | Cyber Attack and Defense – Spezialisierung | 6 | WPM | Siehe MK DEF |
| HPI-SSK-KO | Soft Skills: Kommunikation | 6 | WPM | Siehe MK DEF |
| HPI-SSK-ML | Soft Skills: Management und Leitung | 6 | WPM | Siehe MK DEF |
| HPI-SSKDTB | Soft Skills: Design Thinking Basics | 6 | WPM | Siehe MK DEF |
| HPI-SSKDTA | Soft Skills: Design Thinking Advanced | 6 | WPM | Siehe MK DEF |

LP = Anzahl der Leistungspunkte, PM = Pflichtmodul, WPM = Wahlpflichtmodul

Anlage 2: Exemplarische Studienverlaufspläne

Anlage 2.1 Studienverlaufsplan für das Masterstudium Cybersecurity (Beginn Wintersemester)

| 1. Semester | 2. Semester | 3. Semester | 4. Semester |
|---|--|--|-----------------------------------|
| HPI-CS-T Security Technologies (6 LP) | HPI-CS-C Advanced Cryptography (6 LP) | HPI-CS-L Security Lab (12 LP) | HPI-MA Masterarbeit (30 LP) |
| HPI-CS-S Systems and Network Security (6 LP) | HPI-CS-A Application Security (6 LP) | | |
| HPI-VT1-K Vertiefungsgebiet 1 (6 LP) | HPI-VT1-T Vertiefungsgebiet 1 (6 LP) | HPI-VT1-S Vertiefungsgebiet 1 (6 LP) | |
| HPI-VT2-K Vertiefungsgebiet 2 (6 LP) | HPI-VT2-T Vertiefungsgebiet 2 (6 LP) | HPI-VT2-S Vertiefungsgebiet 2 (6 LP) | |
| HPI-CS-PE Data Protection and Ethics (6 LP) | HPI-DE-RWM Recht, Wirtschaft, Management (6 LP) | HPI-SSK1 Soft Skills (6 LP) | |

Anlage 2.2 Studienverlaufsplan für das Masterstudium Cybersecurity (Beginn Sommersemester)

| 1. Semester | 2. Semester | 3. Semester | 4. Semester |
|--|---|--|-----------------------------------|
| HPI-CS-C Advanced Cryptography (6 LP) | HPI-CS-T Security Technologies (6 LP) | HPI-CS-L Security Lab (12 LP) | HPI-MA Masterarbeit (30 LP) |
| HPI-CS-A Application Security (6 LP) | HPI-CS-S Systems and Network Security (6 LP) | | |
| HPI-VT1-T Vertiefungsgebiet 1 (6 LP) | HPI-VT1-K Vertiefungsgebiet 1 (6 LP) | HPI-VT1-S Vertiefungsgebiet 1 (6 LP) | |
| HPI-VT2-T Vertiefungsgebiet 2 (6 LP) | HPI-VT2-K Vertiefungsgebiet 2 (6 LP) | HPI-VT2-S Vertiefungsgebiet 2 (6 LP) | |
| HPI-DE-RWM Recht, Wirtschaft, Management (6 LP) | HPI-CS-PE Data Protection and Ethics (6 LP) | HPI-SSK1 Soft Skills (6 LP) | |

Hinweise:

- Der Studienverlaufsplan verwendet die Kürzel der Module aus §6. Zudem bezeichnet HPI-VT1 das erste Vertiefungsgebiet, HPI-VT2 das zweite Vertiefungsgebiet. Zum Beispiel: Mit einem ersten Vertiefungsgebiet HPI-SECA bezeichnet HPI-VT1-K das Modul HPI-SECA-K
- HPI-SSK1 bezeichnet das Wahlpflichtmodul aus dem Bereich Soft Skills