21/26

8. Juli 2026

Amtliches Mitteilungsblatt

Seite

htw.
Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

Herausgeber

Das Präsidium der HTW Berlin

Treskowallee 8

10318 Berlin

Redaktion

Justiziariat

Tel. +49 30 5019-2813

Fax +49 30 5019-2815

HOCHSCHULE FÜR TECHNIK UND WIRTSCHAFT BERLIN

Erste Ordnung zur Änderung der Studien- und Prüfungsordnung für den englischsprachigen Bachelorstudiengang

Cyber Security and Business (CSB)

Bachelor of Science (B.Sc.)

im Fachbereich Informatik, Kommunikation und Wirtschaft vom 15. April 2026

Auf Grund von § 16 Abs. 1 Satz 1 Nr. 1 der Satzung der Hochschule für Technik und Wirtschaft Berlin vom 16. Dezember 2024 (AMBl. HTW Berlin Nr. 12/25) in Verbindung mit § 31 des Gesetzes über die Hochschulen im Land Berlin (Berliner Hochschulgesetz - BerlHG) in der Fassung der Bekanntmachung vom 26. Juli 2011 (GVBl. S. 378), zuletzt geändert durch Artikel 1 des Gesetzes vom 21. Januar 2026 (GVBl. S. 23), hat der Fachbereichsrat des Fachbereiches Informatik, Kommunikation und Wirtschaft der HTW Berlin am 15. April 2026 die folgende Erste Ordnung zur Änderung der Studien- und Prüfungsordnung für den Bachelorstudiengang Cyber Security and Business vom 11. Oktober 2023 (AMBl. HTW Berlin Nr. 18/24), beschlossen:[*]

Artikel 1

Nr. 1

Diese Änderungsordnung gilt für alle Studierenden des englischsprachigen Bachelorstudiengangs Cyber Security and Business, die ab dem Wintersemester 2024/25 immatrikuliert wurden.

Nr. 2

Anlage 3 Wahlpflichtmodule

Die „Anlage 3 Wahlpflichtmodule“ wird ersetzt durch:

„**Anlage 3 Wahlpflichtmodule**

Angebot für die Wahlpflichtmodule 1 bis 4

[*] Bestätigt durch das Präsidium der Hochschule für Technik und Wirtschaft Berlin am 13. Mai 2026.

Den Studierenden werden für die Wahlpflichtmodule B24 Wahlpflichtmodul 1, B25 Wahlpflichtmodul 2, B30 Wahlpflichtmodul 3 und B31 Wahlpflichtmodul 4 in jedem Semester in der Regel vier Module angeboten. Aus den angebotenen Modulen können im 4. und 5. Fachsemester vier Module im Umfang von 20 ECTS-Leistungspunkten gewählt werden. Studierende bekommen diejenigen Module mit Zuordnung zur jeweiligen Vertiefung im Zeugnis ausgewiesen, die sie aus dem Wahlpflichtangebot im Umfang von 20 ECTS-Leistungspunkten absolviert haben. Wurde in einer Vertiefung kein Modul erfolgreich absolviert, wird diese nicht ausgewiesen.

Die Zuordnung der Module zu den Vertiefungen und die Voraussetzungen sind in der nachfolgenden Tabelle dargestellt.

Der oder die Studiengangssprecher*in entscheidet rechtzeitig darüber welche Vertiefungen und welche Module pro Vertiefung angeboten werden. Auf Grund aktueller Entwicklungen kann der Fachbereichsrat weitere Wahlpflichtmodule beschließen.

Nr.	**Modulbezeichnung**	**Form**	**SWS**	**NSt**	**NV**	**EV**	**FOR**	**CIKR**	**DLT**	**Comprehensive**
B110	Forensics in Operating Systems	PCÜ	4	1b	-	B9	X			
B111	Analysis Methods for Forensic Data	PCÜ	4	1a	-	-	X			
B112	Forensics Psychology	PÜ	4	1a	-	-	X			
B113	Digital Investigation	PCÜ	4	1b	-	B16	X			
B114	Testing & Hacking	PCÜ	4	1b	-	B10				X
B115	Current Topics in Forensics	PÜ	4	1a	-	-	X			
B130	Critical Infrastructure Protection	PÜ	4	1b	-	B3		X		
B131	Security Operation (SOC)	PCÜ	4	1b	-	B10, B16		X		
B132	Handling Specific Risks	PÜ	4	1b	-	B17		X		
B134	Change Management (IT & HR)	PS	4	1b	-	B22				X
B135	Current Topics in CIKR	PÜ	4	1a	-	-		X		
B150	Fundamentals of Blockchain-Technology/DLT	PCÜ	4	1b	-	B14			X	
B151	Project Management	PS	4	1a	-	-			X	

B152	Blockchain Business Development	PÜ	4	1b	-	B15			X	
B153	Blockchain Security	PCÜ	4	1b	-	B9			X	
B155	Current Topics in Blockchain-Technology	PÜ	4	1b	-	B22			X	
B200	Emergency Management & Psychological Aspects	PÜ	4	1a	-	-				X
B201	Security Awareness	PÜ	4	1a	-	-				X”

Nr. 3

Anlage 6 Lernergebnisse und Kompetenzen für jedes Modul

Die Lernergebnisse und Kompetenzen für das Modul B21 Network and System Security werden ersetzt durch:

“Modulbezeichnung	**B21 Network and System Security**
Lernergebnisse und Kompetenzen	Die Studierenden • können grundlegende Kenntnisse der Kryptologie (vgl. Modul B14) auf kryptographische Protokolle anwenden und diese im Hinblick auf Sicherheitsziele analysieren. • haben ein tiefgreifendes Verständnis von modernen kryptographischen Netzwerkprotokollen und können Angriffe auf diese nachvollziehen. • können Spezifikationen komplexer Protokolle lesen und interpretieren, um für ein gegebenes Sicherheitsniveau geeignete Konfigurationen und Algorithmen auszuwählen. • sind in der Lage, komplexe Netzwerke und Systeme zu abstrahieren, um eine Sicherheitsanalyse durchzuführen. • wenden die grundlegenden Strategien und Gegenmaßnahmen zur Absicherung von Netzwerken und Systemen selbstständig an. Die Studierenden können • geeignete Protokolle, Parameter und Algorithmen auswählen, um definierte Sicherheitsziele zu erreichen. • Netzwerke und Systeme systematisch im Hinblick auf Sicherheitsziele analysieren. • ihre Kenntnisse über Angriffstechniken nutzen, um mögliche Angriffsvektoren aufzuzeigen.

	• angemessene Gegenmaßnahmen auswählen, um die Sicherheit von Netzwerken und Systemen zu erhöhen.“

Artikel 2

Diese Ordnung tritt am Tage nach ihrer Veröffentlichung im Amtlichen Mitteilungsblatt der HTW Berlin mit Wirkung vom 1. Oktober 2026 in Kraft.

HOCHSCHULE FÜR TECHNIK UND WIRTSCHAFT BERLIN

First Amendment to the Study and Examination Regulations for the English-language Bachelor's degree programme

Cyber Security and Business (CSB)

Bachelor of Science (B.Sc.)

at the School of Computing, Communication and Business from the 15th of April 2026

On the basis of § 16, section 1, sentence 1, no. 1 of the Statutes of the Hochschule für Technik und Wirtschaft Berlin (Berlin University of Applied Sciences - HTW Berlin) dated the 16th of December 2024 (HTW Berlin Official Information Circular No. 12/25) in connection with § 31 of the BerlHG in the edition dated the 26th of July 2011 (Law and Official Gazette p. 378), last amended by Article 1 of the Act of the 21st of January 2026 (Law and Official Gazette p. 23), the Faculty Council of Faculty 4, School of Computing, Communication and Business of HTW Berlin, passed the following First Amendment to the Study and Examination Regulations for the Bachelor's Degree Programme Cyber Security and Business dated the 11th of October 2023 (HTW Berlin's Official Information Circular No. 18/24) on the 15th of April 2026:[*]

Article 1

No. 1

This amendment regulation applies to all students of the English-language Bachelor's degree programme Cyber Security and Business who have been enrolled since the winter semester 2024/25.

No. 2

Annex 3 Elective Modules

"Annex 3 Elective Modules" is replaced by:

"**Annex 3 Elective Modules**

[*]Confirmed by the Executive Committee of the Hochschule für Technik und Wirtschaft Berlin on the 13th of May 2026. (Only the original German version is binding).

Options for Elective Modules 1 to 4

Each semester, students are generally offered a choice of four modules for the elective modules B24 (Elective Module 1), B25 (Elective Module 2), B30 (Elective Module 3) and B31 (Elective Module 4). Four modules totalling 20 ECTS credits can be selected from the modules offered in the 4th and 5th semesters. Students receive a certificate showing the modules that they have completed from the elective programme amounting to 20 ECTS credits assigned to the respective specialisation. If no module has been successfully completed in the context of a specialisation, this is not shown.

The assignment of modules to the respective specialisations and their prerequisites are shown in the following table.

The programme representative decides which specialisations and which modules are offered for each specialisation in due time. The Faculty Council may decide on further elective modules according to current developments.

No.	Module Designation	Form	WS H	Lev	CP	RP	FOR	CIKR	DLT	Comprehensive
B110	Forensics in Operating Systems	PCE	4	1b	-	B9	X			
B111	Analysis Methods for Forensic Data	PCE	4	1a	-	-	X			
B112	Forensic-Psychology	PE	4	1a	-	-	X			
B113	Digital Investigation	PCE	4	1b	-	B16	X			
B114	Testing & Hacking	PCE	4	1b	-	B10				X
B115	Current Topics in Forensics	PE	4	1a	-	-	X			
B130	Critical Infrastructure Protection	PE	4	1b	-	B3		X		
B131	Security Operation (SOC)	PCE	4	1b	-	B10, B16		X		
B132	Handling Specific Risks	PE	4	1b	-	B17		X		
B134	Change Management (IT & HR)	PS	4	1b	-	B22				X
B135	Current Topics in CIKR	PE	4	1a	-	-		X		
B150	Fundamentals of Blockchain Technology/DLT	PCE	4	1b	-	B14			X	
B151	Project Management	PS	4	1a	-	-			X	

B152	Blockchain Business Development	PE	4	1b	-	B15			X	
B153	Blockchain Security	PCE	4	1b	-	B9			X	
B155	Current Topics in Blockchain-Technology	PE	4	1b	-	B22			X	
B200	Emergency Management & Psychological Aspects	PE	4	1a	-	-				X
B201	Security Awareness	PE	4	1a	-	-				X”

No. 3

Annex 6 Learning Outcomes and Competences for each Module

The outcomes and competencies for the module B21 Network and System Security are replaced by:

“Module Designation	**B21 Network and System Security**
Learning Outcomes and Competences	The students • are able to apply a basic understanding of cryptology (see Module B14) to cryptographic protocols and analyse them in terms of security objectives. • have a thorough understanding of modern cryptographic network protocols and are able to understand and reconstruct attacks on them. • are able to read and interpret the specifications of complex protocols in order to select appropriate configurations and algorithms for a given security level. • are able to abstract complex networks and systems in order to carry out a security analysis. • apply the basic strategies and countermeasures for securing networks and systems independently. The students are able to • select appropriate protocols, parameters and algorithms in order to achieve defined security objectives. • systematically analyse networks and systems with regard to security objectives. • use their knowledge of attack techniques to identify potential attack vectors. • select appropriate countermeasures to enhance the security of networks and systems.”

Article 2

This regulation comes into force on the day after its publication in HTW Berlin's Official Information Circular with effect from the 1st of October 2026.