ALLEGATO
MODELLO DI SYLLABUS (SCHEDA DI INSEGNAMENTO) - IT

ANNO ACCADEMICO 2021/22	
1. Docente responsabile dell'Insegnamento	Andrea Monti – Docente a contratto per elevata qualificazione
[1.1 Docenti titolari di singoli moduli all'interno dell'insegnamento]	
2. Insegnamento	Cybersecurity Contracts
3. Corso di Studio e Anno Regolamento	Laurea Magistrale in Giurisprudenza (LMG-01) Anno accademico 202-2021-2022
4. Numero CFU	6
5. Settore Scientifico Disciplinare	IUS-01
6. Tipo di Attività	A scelta dello studente
7. Anno Corso	V
8. Lingua di Insegnamento	Inglese
9. Contenuti del Corso ed eventuale articolazione in moduli con indicazione del soggetto titolare dei singoli moduli se diverso dal responsabile del Corso	Il corso di Cybersecurity Contracts è diviso in due parti. Parte I (Evoluzione tecnica, economica e normativa della cybersecurity) – Fondamenti di sviluppo software, dei sistemi informativi e delle informazioni – Il fenomeno del hacking dagli USA all'Europa – La nascita del mercato della sicurezza informatica – Ruolo e responsabilità delle software-house nella creazione delle vulnerabilità – La diffusione dell'internet, la mutazione delle minacce e il cambiamento delle tipologie di servizio – Cybersecurity, Blockchain – Tassonomia dei profili pubblicistici e privatistici della Cybersecurity – Cybersecurity, ordine pubblico, sicurezza nazionale e diritti – Cybersecurity e proprietà intellettuale – Responsabilità (extra)contrattuale: limiti e impatto dell'AI, – Il ruolo delle certificazioni e degli standard ai fini della corretto adempimento delle obbligazioni contrattuali, – Cybersecurity e compliance aziendale Parte II (Modelli contrattuali) – Software development/Secure programming – Internet Access e clausole di sicurezza – SaaS e clausole di sicurezza – Security Operation Center (SOC) – Managed Security Service – Penetration Test/Vulnerability Assessment – Red Teaming/Offensive Security

	– Security Audit – Non Disclosure Agreement – Cybersecurity SmartContract
10. Testi di Riferimento	Monti, A. Wacks, R. *National Security in the New World Order Government and the Technology of Information*, Routledge 2022 Tollen, D. *The Tech Contracts Handbook: Software Licenses, Cloud Computing Agreements, and Other IT Contracts for Lawyers and Businesspeople* American Bar Association, 2021
11. Obiettivi Formativi	L'obiettivo del corso è fornire allo studente le competenze per: – comprendere le dinamiche di mercato del settore della cybersecurity – individuare gli elementi tecnici rilevanti ai fini della definizione di un contratto di cybersecurity, – definire le obbligazioni contrattuali in funzione del ruolo rivestito (committente o fornitore di servizi di sicurezza), analizzare e sviluppare clausole e contrattuali attinenti alla cybersecurity sia dalla prospettiva del fornitore di questi servizi, sia dal punto di vista dell'utenza aziendale e istituzionale
12. Risultati di Apprendimento Attesi	Conoscenza e comprensione All'esito della frequenza del corso ci si aspetta che lo studente sia in grado di riconoscere le diverse tipologie di servizio, comprenderne in linea generale il contenuto tecnico. Capacità di applicare conoscenza e comprensione Lo studente dovrebbe essere in grado di progettare l'architettura di un contratto di cybersecurity e definire, dal punto di vista del fornitore o dell'utilizzatore, le criticità contrattuali. Abilità comunicative Lo studente dovrebbe essere in grado di spiegare la ratio delle scelte compiute nella progettazione di un contratto di cybersecurity e del contenuto delle singole clausole. Capacità di apprendimento Lo studente dovrebbe avere appreso il metodo per aggiornare in autonomia le proprie conoscenze e individuare nuove aree di conoscenza utili a integrare le capacità raggiunte.
13. Prerequisiti ed Eventuali Propedeuticità	Non sono richiesti particolari prerequisiti ma il possesso di fondamenti di informatica e telecomunicazioni sarebbero auspicabili.
14. Metodi Didattici	Video/Audio lezioni assistite da slide e materiale di approfondimento e questionario di autovalutazione per ogni singolo intervento didattico. Gli studenti hanno, inoltre, la possibilità di interagire a distanza con il docente tramite mail, chat o webconference
15. Agenda 2030, UN Sustainable Development Goals	**4 Istruzione di qualità**: fornire agli studenti conoscenze e competenze su temi che agevolano l'ingresso nel mondo del lavoro e della consulenza nel settore high-tech. **9 Imprese, innovazione e infrastrutture**: contribuire al miglioramento dell'ecosistema cybersecurity elevando i livelli di attenzione in imprese ed istituzioni. **16 Pace, giustizia e istituzioni solide**: rendere più sicure aziende ed istituzioni e ridurre i rischi di failure delle infrastrutture nazionali
16. Altre Informazioni	

17. Modalità di Verifica dell'Apprendimento	La prova finale consiste in un esame scritto con 31 domande a risposta multipla. Ogni risposta esatta è valutata con un punto. Le risposte sbagliate non abbassano la valutazione. L'esame è superato con 18 risposte esatte che attribuiscono 18/30. La lode è attribuita con 31 risposte esatte.
18. Programma Esteso	1) Fondamenti di sviluppo software, architetture dei sistemi informativi e delle informazioni – Architetture di calcolatori, linguaggi di programmazione e framework di sviluppo, – Il processo di sviluppo software: analisi, scrittura, implementazione – La gestione degli errori e il secure programming – Struttura e funzionamento di una rete informatica – Architettura centralizzata e distribuita (cloud-computing, edge computing) – Ruolo e funzione dei protocolli di rete – Struttura e funzionamento di una rete di telecomunicazioni 2) Il fenomeno del hacking dagli USA all'Europa – Il ruolo dell'accademia e della società civile nella nascita del fenomeno hacking, – La rottura del monopolio delle multinazionali IT e il "doppio binario" nell'approccio al software proprietario (Apple/Microsoft) e libero (Stallman/Perens) – Le caratteristiche del hacking europeo e italiano 3) La nascita del mercato della sicurezza informatica – Le prime forme di attacchi informatici: the Internet Worm, la diffusione di virus, gli accessi abusivi a istituzioni e grandi aziende, 4) La diffusione dell'internet, la mutazione delle minacce e il cambiamento delle tipologie di servizio – La diffusione dell'internet e l'ampliamento delle vittime potenziali – Il ruolo degli Internet Provider come garanti della sicurezza della rete – La nascita dei SOC – Il mercato dei security appliance – I Managed Security Service – Cybersecurity e Blockchain 5) Profili pubblicistici della Cybersecurity – Cybersecurity, ordine pubblico, sicurezza nazionale e diritti fondamentali – Il perimetro nazionale di sicurezza cibernetica 6) Profili privatistici della Cybersecurity – L'impatto della definizione pubblicistica di Cybersecurity sul regime civilistico (in particolare: sulla necessità di ampliare la definizioni normativa) – L'identificazione delle parti – La natura, il contenuto e limiti delle obbligazioni (in particolare, sul tema della esigibilità della prestazione) – Il ruolo della proprietà intellettuale nell'adempimento (in particolare, sul ruolo delle licenze "libere"),

	7) Responsabilità (extra)contrattuale – Ruolo e responsabilità delle software-house nella creazione delle vulnerabilità – Ruolo e responsabilità degli Internet Provider e degli operatori di comunicazione 8) Il ruolo delle certificazioni e degli standard ai fini della corretto adempimento delle obbligazioni contrattuali – Le certificazioni ISO e gli standard NIST Il ruolo della Cybersecurity nella compliance aziendale (Modello organizzativo 231, GDPR, Sicurezza sui luoghi di lavoro)
19. Contatti e orario di ricevimento	Preferibilmente online, previo appuntamento da concordare volta per volta scrivendo all'indirizzo amonti@unich.it

MODELLO DI SYLLABUS (SCHEDA DI INSEGNAMENTO) - ENG

unidav.it UNIVERSITÀ TELEMATICA 'LEONARDO DA VINCI'	
ACADEMIC YEAR 2021/22	
1. Regular Teacher	Andrea Monti – Adjunct Professor
1.1[Lecturer/s assigned to specific single modules within the course]	
2. Course name	
3. Course Programme and Year of Regulations	Faculty of Law - Academic Year 21-22
4. Number of Credits	6
5. Scientific Disciplinary Sector	IUS-01
6. Type of activity	Optional exam
7. Year of Course	V
8. Teaching language	English
9. Contents of the Course and possible articulation in modules with indication of the relative appointee/s if different from the regular teacher of the Course	The Cybersecurity Contracts course is divided into two parts. **Part I (Technical, Economic, and Regulatory Evolution of Cybersecurity)** - Fundamentals of software development, information systems and information - The phenomenon of hacking from the USA to Europe - The birth of the cybersecurity market - Role and responsibility of the software-house in the creation of vulnerabilities - The diffusion of the Internet, the mutation of threats and the change of service types - Cybersecurity, Blockchain - Taxonomy of the public and private profiles of cybersecurity - Cybersecurity, public order, national security and rights - Cybersecurity and intellectual property - (Extra)contractual liability: limits and impact of AI, - The role of certifications and standards for the correct fulfillment of contractual obligations, - Cybersecurity and corporate compliance **Part II (Contractual models)** - Software development/Secure programming - Internet Access and security clauses - SaaS and security clauses - Security Operation Center (SOC) - Managed Security Service - Penetration Test/Vulnerability Assessment - Red Teaming/Offensive Security - Security Audit - Non-Disclosure Agreement - Cybersecurity SmartContract

10. Reference Books and Texts	Monti, A. Wacks, R. *National Security in the New World Order Government and the Technology of Information*, Routledge 2022 Tollen, D. *The Tech Contracts Handbook: Software Licenses, Cloud Computing Agreements, and Other IT Contracts for Lawyers and Businesspeople* American Bar Association, 2021
11. Learning objectives	The aim of the course is to provide students with the skills to: - understand the market dynamics of the cybersecurity sector - identify the technical elements relevant to the definition of a cybersecurity contract - define the contractual obligations according to the role played (client or security service provider) - analysing and developing clauses and contracts relating to cybersecurity, both from the perspective of the provider of these services, and from the point of view of corporate and institutional users
12. Expected Learning outcomes	Knowledge and Understanding At the end of course attendance, the student is expected to be able to recognize the different types of services, understand their technical content in general. Ability to apply knowledge and understanding The student should be able to design the architecture of a cybersecurity contract and define, from the point of view of the provider or user, the critical contractual issues. Communication skills The student should be able to explain the rationale for the choices made in the design of a cybersecurity contract and the content of the individual clauses. Learning skills The student should have learned the method to independently update their knowledge and identify new areas of knowledge useful to integrate the skills achieved.
13. Possible necessary pre-requisites or preparatory activity/ies	No particular prerequisites are required, but basic IT and telecommunications skills would be desirable.
14. Teaching Methods	Video/audio lectures assisted by slides and in-depth material and a self-assessment questionnaire for each lecture. Students also have the possibility of interacting with the lecturer via e-mail, chat or webconference.
15. Agenda 2030, Sustainable development Goals	**4 Quality education**: provide students with knowledge and skills on topics that facilitate to apply working positions or provide consultancy services in the high-tech sector. **9 Business, innovation and infrastructure** - help improve the cybersecurity ecosystem by raising the bar in businesses and public institutions. **16 Peace, justice and strong institutions** - making businesses and public institutions more secure and reducing the risk of failure of national infrastructure
16. Other information	
17. Assesment Methods	The final examination consists of a written test with 31 multiple-choice questions. Each correct answer is marked with one point. Wrong answers do not lower the final result . The examination is passed with 18 correct answers giving 18/30. Cum Laude is awarded for 31 correct answers.
18. Full programme	Extended programme

	1) Fundamentals of software development, information systems and information architectures - Computer architectures, programming languages and development frameworks, - The software development process: analysis, writing, implementation - Error management and secure programming - Structure and functioning of a computer network - Centralised and distributed architecture (cloud computing, edge computing) - Role and function of network protocols - Structure and functioning of a telecommunications network 2) The hacking phenomenon from the USA to Europe - The role of academia and civil society in the birth of the hacking phenomenon, - The breaking of the monopoly of the IT multinationals and the "double binary" approach to proprietary software (Apple/Microsoft) and free software (Stallman/Perens) - The characteristics of European and Italian hacking 3) The birth of the computer security market - The first forms of computer attacks: the Internet Worm, the spread of viruses, abusive accesses to institutions and large companies, 4) The spread of the Internet, the mutation of threats and the change in types of service - The spread of the Internet and the expansion of potential victims - The role of Internet Providers as guarantors of network security - The birth of the SOC - The security appliance market - Managed Security Services - Cybersecurity and Blockchain 5) Public profiles of cybersecurity - Cybersecurity, public order, national security and fundamental rights - The national cyber security perimeter 6) Private Profiles of Cybersecurity - The impact of the public definition of cybersecurity on the civil law regime (in particular: on the need to broaden the regulatory definitions) - The identification of the parties - The nature, content and limits of the obligations (in particular, on the issue of the collectability of the performance) - The role of intellectual property in performance (in particular, on the role of "free" licences), 7) (Extra) contractual responsibility - Role and responsibility of software companies in creating vulnerabilities - Role and responsibility of Internet Providers and communication operators 8) The role of certifications and standards for the correct fulfilment of contractual obligations - ISO certifications and NIST standards - The role of cybersecurity in corporate compliance (Organisational Model 231, GDPR, Safety in the workplace)

19. Contacts and Professors' office hours	Preferably online, by appointment to be agreed from time to time by writing to amonti@unich.it