SCHEDA DI INSEGNAMENTO - IT

ANNO ACCADEMICO 2023/24	
1. Docente responsabile dell'Insegnamento	Andrea Monti – docente a contratto
[1.1 Docenti titolari di singoli moduli all'interno dell'insegnamento]	
2. Insegnamento	Cybersecurity contract
3. Corso di Studio e AnnoRegolamento	CdL magistrale a ciclo unico in Giurisprudenza – Regolamento didattico a.a. 2023-2024.
4. Numero CFU	8
5. Settore Scientifico Disciplinare	IUS/01 – Diritto privato
6. Tipo di Attività	C
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 edelle informazioni – Il fenomeno del hacking dagli USA all'Europa – La nascita del mercato della sicurezza informatica – Ruolo e responsabilità delle software-house nella creazionedelle vulnerabilità – La diffusione dell'internet, la mutazione delle minacce e ilcambiamento 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 Smart Contract

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, CloudComputing Agreements, and Other IT Contracts for Lawyers andBusinesspeople* 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 dellacybersecurity – individuare gli elementi tecnici rilevanti ai fini delladefinizione di un contratto di cybersecurity, – definire le obbligazioni contrattuali in funzione del ruolorivestito (committente o fornitore di servizi di sicurezza), – analizzare e sviluppare clausole e contrattuali attinenti allacybersecurity sia dalla prospettiva del fornitore di questi servizi, sia dal punto di vista dell'utenza aziendale e istituzionale
12. Risultati di ApprendimentoAttesi	All'esito della frequenza del corso ci si aspetta che lo studente sia in grado di riconoscere le diverse tipologie di servizio, comprenderne inlinea generale il contenuto tecnico e individuare, dal punto di vista del fornitore o dell'utilizzatore, le criticità contrattuali.
13. Prerequisiti ed eventuali Propedeuticità	Non sono richiesti particolari prerequisiti ma il possesso di fondamenti di informatica e telecomunicazioni sarebbero auspicabili.
14. Metodi Didattici	In ossequio alle Linee guida sulla didattica di Ateneo, la *didattica erogativa* comprende videolezioni preregistrate dal docente che illustrano i contenuti del Corso. Ciascuna videolezione trova completamento nel materiale testuale di approfondimento (*slide* e dispense). La *didattica interattiva* prevede un test di autovalutazione composto da domande a risposte multipla che consentono agli studenti di accertare la comprensione e il grado di conoscenza acquisita dei contenuti di ciascuna lezione. Infine, ai fini della preparazione e per consentire allo Studente di esercitarsi in vista del superamento dell'esame di profitto, è altresì disponibile un *database* di domande aperte e chiuse. La *didattica interattiva* si completa con un *forum* didattico contenente almeno un *thread* per ogni CFU; a questo si aggiunge almeno un'altra *e-tivity* (strutturata, individuale o collaborativa) per ogni CFU che saranno organizzate e fruibili nelle modalità indicate sulla piattaforma *e-learning* del Corso. I predetti contenuti didattici sono resi disponibili e accessibili secondo i tempi previsti nel GANTT del Percorso formativo allegato al Regolamento didattico del presente anno accademico.
15. Agenda 2030, UN Sustainable Development	Obiettivi 4, 8 e 9
16. Altre Informazioni	
17. Modalità di Verifica dell'Apprendimento	La verifica dell'apprendimento avverrà mediante una prova scritta, secondo le disposizioni del Regolamento di Ateneo per gli esami scritti dei Corsi di laurea. In particolare, l'esame consiste in una prova scritta composta da ventuno domande a risposta chiusa e di tre domande a risposta aperta. A ogni risposta chiusa corrisponde un 1 punto se esatta, 0 punti se errata o non data. Le risposte aperte valgono da 0 a 3 punti, secondo i seguenti valori: 0, insufficiente; 1, sufficiente; 2, buono; 3, ottimo.

	Nella valutazione delle risposte aperte, si terrà conto dei seguenti aspetti: 1) grado di conoscenza e approfondimento dei contenuti; 2) qualità dell'argomentazione; 3) uso del linguaggio tecnico-disciplinare. Per la partecipazione alle *e-tivities* del Corso sarà attribuito un punteggio da 0 a 2 punti, secondo i seguenti valori: 0, partecipazione insufficiente; 1, partecipazione sufficiente; 2, partecipazione attiva e propositiva. Tale punteggio sarà sommato al voto finale. Il voto finale è espresso in trentesimi e va da 1 a 30 con lode, secondo i seguenti intervalli: 1-17, insufficiente; 18-21, sufficiente; 22-24, discreto; 25-27, buono; 28-29, molto buono; 30-30 con lode, eccellente (sezione da mantenere o cancellare, secondo le esigenze del/la docente).
18. Programma Esteso	1) Fondamenti di sviluppo software, architetture dei sistemiinformativi e delle informazioni – Architetture di calcolatori, linguaggi di programmazionee 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 ditelecomunicazioni 2) Il fenomeno del hacking dagli USA all'Europa – Il ruolo dell'accademia e della società civile nella nascitadel 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 InternetWorm, la diffusione di virus, gli accessi abusivi a istituzioni e grandi aziende, 4) La diffusione dell'internet, la mutazione delle minacce e ilcambiamento delle tipologie di servizio – La diffusione dell'internet e l'ampliamento delle vittimepotenziali – Il ruolo degli Internet Provider come garanti dellasicurezza 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 ediritti fondamentali – Il perimetro nazionale di sicurezza cibernetica 6) Profili privatistici della Cybersecurity – L'impatto della definizione pubblicistica di Cybersecurity sul regime civilistico (in particolare: sullanecessità 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 (inparticolare, sul ruolo delle licenze "libere"), 7) Responsabilità (extra)contrattuale – Ruolo e responsabilità delle software-house nellacreazione delle vulnerabilità – Ruolo e responsabilità degli Internet Provider e deglioperatori di comunicazione 8) Il ruolo delle certificazioni e degli standard ai fini della correttoadempimento delle obbligazioni contrattuali – Le certificazioni ISO e gli standard NIST – Il ruolo della Cybersecurity nella compliance aziendale (Modello organizzativo 231, GDPR, Sicurezza sui luoghidi lavoro)
19. Contatti e orario di ricevimento	Su appuntamento da concordare volta per volta scrivendoall'indirizzo amonti@unich.it.

(SCHEDA DI INSEGNAMENTO) -
ENG

ACADEMIC YEAR2022/23	
1. Regular Teacher	Andrea Monti
1.1[Lecturer/s assigned to specific single modules withinthe course]	
2. Course name	
3. Course Programme andYear of Regulations	Law - Academic Year 22-23
4. Number of Credits	8
5. Scientific DisciplinarySector	IUS-01
6. Type of activity	C
7. Year of Course	V
8. Teaching language	English
9. Contents of the Course and possible articulation in modules with indication of therelative appointee/s if differentfrom the regular teacher of theCourse	The Cybersecurity Contracts course is divided into two parts.Part I (Technical, economic and regulatory evolution of cybersecurity) - Fundamentals of software, information systems and informationdevelopment - The hacking phenomenon from the USA to Europe - The birth of the cybersecurity market - Role and responsibility of software companies in creatingvulnerabilities - The spread of the Internet, the mutation of threats and the change intypes of service - 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 fulfilment ofcontractual 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 acybersecurity 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	At the end of the course, students are expected to recognise the different types of service, to understand their technical content in general terms and to identify critical contractual issues from theperspective of the provider or user.
13. Possible necessary pre-requisites or preparatoryactivity/ies	No particular prerequisites are required, but basic IT andtelecommunications skills would be desirable.
14. Teaching Methods	In accordance with the Teaching Guidelines, teaching methods includes pre-recorded video-lessons that illustrate the course content. Each video-lesson is completed by in-depth textual material (slides and handouts). Interactive teaching methods includes a self-assessment test consisting of multiple-choice questions that allow students to ascertain the level of their understanding and of their knowledge of the contents of each lesson. Finally, A database of open-ended questions and multiple-choice questions is also available in order to prepare students for the exam. Interactive teaching methods are completed with a didactic forum containing at least one thread for each CFU; in addition to this, at least one other *e-tivity* for each CFU will be organised within the e-learning platform. The aforementioned teaching contents are made available and accessible according to the timescales set out in the GANTT of the Teaching Activities annexed to the Teaching Regulation of the present academic year.
15. Agenda 2030, Sustainable development Goals	Goals n. 4, 8 and 9.
16. Other information	
17. Assessment Methods	The learning assessment will take place by means of a written test, in accordance with the provisions of the University Regulations for written examinations of degree courses. In particular, the examination consists of a written test comprising twenty-one closed-answer questions and three open-answer questions. Each closed answer corresponds to 1 point if correct, 0 points if incorrect or not given. Open answers are worth between 0 and 3 points, according to the following values: 0, insufficient; 1, sufficient; 2, good; 3, excellent. In the evaluation of open answers, the following aspects will be taken into account: 1) degree of knowledge and depth of content; 2) quality of argumentation; 3) use of technical-disciplinary language.

	A mark from 0 to 2 points will be attributed for participation in the e-activities of the Course, according to the following values: 0, insufficient participation; 1, sufficient participation; 2, active and proactive participation. This score will be added to the final grade.The final grade is expressed in thirtieths and ranges from 1 to 30 with honours, according to the following intervals: 1-17, insufficient; 18-21, sufficient; 22-24, fair; 25-27, good; 28-29, very good; 30-30 with honours, excellent.
18. Full programme	Extended programme 1) Fundamentals of software development, information systems andinformation architectures - Computer architectures, programming languages and developmentframeworks, - 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 hackingphenomenon, - 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 spreadof viruses, abusive accesses to institutions and large companies, 4) The spread of the Internet, the mutation of threats and the change intypes 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 theissue of the collectability of the performance) - The role of intellectual property in performance (in particular, on therole 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 ofcontractual 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	Upon request by email at amonti@unich.it the student can arrange ameeting with the teacher.