

	<b>UČNI NAČRT PREDMETA/COURSE SYLLABUS</b>
<b>Predmet</b>	<b>Varnostne politike</b>
<b>Course title</b>	<b>Information Security Policies</b>

<b>Študijski program in stopnja</b> <b>Study programme and level</b>	<b>Študijska smer</b> <b>Study field</b>	<b>Letnik</b> <b>Academic year</b>	<b>Semester</b> <b>Semester</b>
Poslovna informatika / I. stopnja	Računalništvo informatika	3. letnik	5.
Business Informatics / 1 <sup>st</sup> Cycle	Computer and Information Science	3 <sup>rd</sup> year	5 <sup>th</sup>

**Vrsta predmeta/Course type**

modularni / module

**Univerzitetna koda predmeta/University course code**

I\_RI\_3\_M2\_UN3

<b>Predavanja</b> <b>Lectures</b>	<b>Seminar</b> <b>Seminar</b>	<b>Sem. vaje</b> <b>Tutorial</b>	<b>Lab. vaje</b> <b>Laboratory work</b>	<b>Teren. vaje</b> <b>Field work</b>	<b>Samost. delo</b> <b>Individ. work</b>	<b>ECTS</b>
30			30		90	6

**Nosilec predmeta/Lecturer:**

doc. dr. Sebastian Lahajnar

**Jeziki/ Languages:**

**Predavanja/Lectures:** slovenski/Slovenian

**Vaje/Tutorial:**

slovenski/Slovenian

**Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:**

**Prerequisites:**

- Pogoj za vključitev v delo je vpis v tretji letnik študija.
- Študent mora pred izpitom pripraviti in predstaviti seminarsko nalogo.

- The prerequisite for participation is enrolment in the third year of study.
- Students have to successfully prepare and present a seminar paper before the examination.

**Vsebina:**

**Content (Syllabus outline):**

- *Temeljni pojmi s področja varovanja informacij. Zaupnost, razpoložljivost, celovitost informacij.*
- *Grožnje informacijski varnosti. Zlonamerna programska oprema, zlonamerni in nedovoljeni postopki, socialni inženiring, zanesljivost IS.*
- *Ocena tveganja. Identifikacija sredstev in ocena njihove vrednosti,*

- *Basic concepts in the field of information security. Confidentiality, availability, integrity of information.*
- *Threats to information security. Malware, malicious and illegal procedures, social engineering, IS reliability.*
- *Risk assessment. Identification of resources and assessment of their*

<p>groženje in ranljivosti sredstev, ocena nevarnosti, stopnje tveganja.</p> <ul style="list-style-type: none"> <li>• <i>Program za varovanje informacij. Osebe, postopki, tehnologije.</i></li> <li>• <i>Zakodajni vidiki informacijske varnosti.</i></li> <li>• <i>Mednarodne organizacije in standardi s področja varovanja informacij (ISO 27001, ISO 27002, Cobit).</i></li> <li>• <i>Osnovna vodila za pisanje varnostnih politik.</i></li> <li>• <i>Razvoj politike: definicija, standardi, procedure, ključni elementi politike, vsebina.</i></li> <li>• <i>Izjava o poslanstvu. Poslovni cilji in varnostni cilji, odgovornost za informacijsko varnost, ključne vloge v organizaciji.</i></li> <li>• <i>Specifične varnostne politike in primeri: organizacijska varnost, varnost in nadzor nad sredstvi, osebe, fizična varnost, komunikacije in operativa, nadzor dostopa, razvoj in vzdrževanje programske opreme, poslovanje, skladnost z legalnimi in tehničnimi zahtevami.</i></li> </ul>	<p>value, threats and vulnerabilities, risk of exposure assessment, the degree of risk.</p> <ul style="list-style-type: none"> <li>• <i>Information security program. People, procedures, technologies.</i></li> <li>• <i>Regulatory aspects of information security.</i></li> <li>• <i>International organizations and standards for information security (ISO 27001, ISO 27002, Cobit).</i></li> <li>• <i>Basic guidelines for writing security policies.</i> <i>Policy development: definition, standards, procedures, key elements of policy content.</i></li> <li>• <i>Mission statement. Business objectives and security objectives, the responsibility for information security, key roles in the organization.</i></li> <li>• <i>Specific security policies and examples: organizational security, security and control over resources, personnel, physical security, communication and operations, access control, software development and maintenance, business, legal and technical requirements compliance.</i></li> </ul>
---	--

### **Temeljna literatura in viri/Readings:**

#### **Temeljna literatura/Basic literature**

- Humphreys, E. (2007). Implementing the ISO/IEC 27001 information security management system standard. Boston, London: Artech House.
- Mather, T. (2005). Varovanje informacij. Pasadena.
- Peltier, T. R. (2002). Information Security Policies, Procedures and Standards. Auerbach Publications.
- Standard SIST ISO/IEC 27001: Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve.
- Standard SIST ISO/IEC 27002 Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri upravljanju informacijske varnosti.

#### **Priporočljiva literatura/Recommended literature**

- ISACA. (2012). COBIT 5: a business framework for the governance and management of enterprise IT. Rolling Meadows: ISACA.
- ISACA. (2012). COBIT 5: for information security. Rolling Meadows: ISACA.
- Kostopoulos, G. K., (2013). Cyberspace and cybersecurity. Boca Raton (FL): CRC Press.

**Cilji in kompetence:**

*Učna enota prispeva predvsem k razvoju naslednjih splošnih in specifičnih kompetenc:*

- avtonomnost, (samo)kritičnost, (samo)refleksivnost, samoocenjevanje in prizadevanje za kakovost,
- etična refleksija in zavezanost profesionalni etiki v informatiki, upravljanju in poslovanju,
- razumevanje - področja računalništva in informatike in povezanost s podpodročji, predvsem informatiko v upravljanju in poslovanju,
- sposobnost uporabe informacijsko-komunikacijske tehnologije in sistemov na področju upravljanja in poslovanja,
- razumevanje temeljnih pojmov varovanja informacij,
- poznavanje pomena mednarodne standardizacije s področja varovanja informacij,
- razumevanje pomena sistema za upravljanje varovanja informacij;
- sposobnost ocenjevanja tveganja in določanja sprejemljivega nivoja tveganja.

**Objectives and competences:**

*The learning unit mainly contributes to the development of the following general and specific competences:*

- autonomy, (self-) criticism, (self-) reflexivity, self-evaluation and commitment to quality,
- ethical reflection and commitment to professional ethics in informatics, business and management,
- understanding the field of computer and informatics and its relationship with subfields, especially business and management,
- the ability of using information-communication technologies and systems in the field of business and management,
- understanding basic concepts of information security,
- understanding the importance of international standardization in the field of information security,
- understanding the importance of information security management system,
- the ability of risk assessment and determination of an acceptable risk level.

**Predvideni študijski rezultati:**

Znanje in razumevanje:

*Študent/Študentka:*

- razume koncept varovanja informacij,
- razume pomen in posledice pravilno definirane in ustrezno uveljavljanje varnostne politike,
- pozna zgradbo in postopek razvoja varnostne politike,
- sposob-en/-na je razviti preproste primere krovne (visokonivojske) in podrobne – specifične varnostne politike,
- razume in presega morebitni konflikt med poslovnimi in varnostnimi cilji v organizaciji,
- pozna mednarodne standarde s področja varovanja informacij,
- je sposob-en/-na identifikacije

**Intended learning outcomes:**

Knowledge and understanding:

*Students:*

- understand the concept of information security,
- understand the importance and consequences of the properly defined and deployed security policy,
- are familiar with the structure and the development process of security policy,
- are able to develop simple examples of organizational (high-level) and detailed-specific security policies,
- understand and exceed the potential conflict between business and security objectives of the organization,
- gain knowledge of information

<p>tveganja in grobe ocene stopnje tveganja,</p> <ul style="list-style-type: none"> <li>• je sposob-en/-na spremljati aktualno literaturo s tega področja in kritično ovrednotiti vsebino glede na osvojeno znanje,</li> <li>• v povezavi z drugimi predmeti je sposoben/-na ovrednotiti pomen in potencialne koristi določanja enotnih varnostnih politik v organizaciji in morebitnih organizacijskih sprememb, ki jih to utegne povzročiti.</li> </ul>	<p>security international standards,</p> <ul style="list-style-type: none"> <li>• are capable of identifying risks and rough estimates of the risk levels,</li> <li>• are able to review the current literature in this field and to critically evaluate the content based on the established knowledge,</li> <li>• in conjunction with other courses are capable to evaluate the importance and potential benefits of setting uniform security policies of the organization and any organizational changes that may result.</li> </ul>
---	---

**Metode poučevanja in učenja:**

**Learning and teaching methods:**

<ul style="list-style-type: none"> <li>• <i>predavanja</i> z aktivno udeležbo študentov (razlaga, diskusija, prikaz na računalniku),</li> <li>• <i>laboratorijske vaje</i> (praktična uporaba predstavljenih konceptov, prikaz orodij, tehnologij in dosegljivih aplikacij),</li> <li>• <i>samostojen študij</i> z izdelavo seminarske naloge</li> </ul>	<ul style="list-style-type: none"> <li>• <i>lectures</i> with active participation of students (explanation, discussion, demonstrations on computer),</li> <li>• <i>laboratory work</i> (practical use of presented concepts, presentation of tools, technologies and available applications),</li> <li>• <i>individual study</i> to prepare a seminar paper.</li> </ul>
--	--

**Načini ocenjevanja:**

Delež (v %)  
Weight (in %)

**Assessment:**

<p>Načini:</p> <ul style="list-style-type: none"> <li>• pisni (ustni) izpit</li> <li>• izdelava, predstavitev in zagovor seminarske naloge</li> </ul>	<p>60 40</p>	<p>Types:</p> <ul style="list-style-type: none"> <li>• written (oral) exam</li> <li>• preparation, presentation and defence of the seminar paper</li> </ul>
---	------------------	---