Master of Science
(Cyber Security and Forensic Computing)
An increasing number of organisations are facing significant challenges in the protection of the information assets and their customers’ sensitive information from outside attacks.

Computer forensics, network security and critical infrastructure protection are emerging subfields of computer science that are gaining much attention at present.

Industry surveys show that the number of computer forensic and related professionals has been experiencing double digit growths and it is set to increase. It will thus provide many career opportunities for information technology and computer science graduates.

The School of Computer and Information Science, at the University of South Australia have a diverse range of high quality programs, and none more so than the Master of Science (Cyber Security and Forensic Computing).

This innovative program is the only one of its kind in Australia and covers industry recommended competencies for information assurance. It is designed for professional development of IT practitioners within the Australian Law Enforcement and will lead to exciting careers in this field.

A Master of Science (Cyber Security and Forensic Computing) from UniSA will equip you with the skills, knowledge and experience necessary to meet the high demands in the Australian Defence, security, banking and other commercial and government organisations.

I invite you to review this brochure and contact us to discuss how you can become a part of this exciting new program.
From the Dean of Research

These postgraduate programs have been developed to meet the established Australian Law Enforcement demand for graduates with a Master Degree level in cyber security and forensic computing to establish expertise for the Australian courts.

No other Master Degrees in Australia have been developed around these competencies. The suite of programs prepares students for the workplace by covering industry recommended competencies for information assurance, electronic evidence, forensic computing and critical infrastructure professionals.

Professor Jill Slay
Dean: Research
Division of Information Technology, Engineering and the Environment
University of South Australia

Univeristy of South Australia’s Dean of Research, Professor and Research Leader in Forensic Computing, Professor Jill Slay is a member of the National Information Assurance Training and Certification (NIATEC) Centre which seeks to address the increasing vulnerability of cyber-based disruption and attacks by establishing a federal cyber-corps.

Through collaborative links with NIATEC’s Director Professor Corey Schou and the South Australian Police, this program has been developed to meet the needs of industry.

Program Director and Lecturer Dr Elena Sitnikova is one of the first Certified Security Software Lifecycle Professional (CSSLP) in Australia.

Courses are offered by academics who are active as researchers and practitioners in their field, and who are able to offer the resulting expertise as part of their teaching.

The program is directly supported by the relevant University of South Australia’s research institutes. Strong links with industry and research organisations ensure that the degrees offered are highly relevant to industry employers at local, national and international level.
Founded in 1991 through the amalgamation of some of the State’s most distinguished education facilities, the University of South Australia (UniSA) is a modern, dynamic, accessible international and entrepreneurial institution. It is a leader in educating professionals and conducting research with application in mind.

The teaching and learning environment is shaped by student-engaged learning, integration of real world professional experience, and a set of graduate qualities. The University has an excellent record in the provision of flexible education, online and offshore teaching programs and industry partnerships.

UniSA has five campuses in South Australia, centres of learning in ten other countries and links with more than 75 institutions worldwide.

Giving UniSA its distinct character is the diversity of the student population – over 11,000 of its 34,000 students are international students from over 70 countries.

UniSA is also the first Australian university, together with the Australian National University (ANU) to forge links through a new collaborative arrangement to work to build on their respective strengths.

The Division of Information, Technology, Engineering and the Environment (ITEE) in which this program is located is at the cutting edge of teaching, research and knowledge transfer in areas of significance to modern society.

Information Technology has not only changed the way business is conducted, it has transformed the way that we live. It is an integral part of every organisation, enabling us to gain unprecedented efficiencies and create value through business model innovation.

The School of Computer and Information Science is the largest ICT tertiary provider in South Australia and one of the largest, most exciting schools in Australia. Crucial to the success of the School is its active involvement with business through the Industry Alliance Program (IAP).
A pathway for professional staff in law enforcement and other professions to increase their capability in cyber security and forensic computing.

- Opportunity to undertake postgraduate study in the field of cyber security and forensic computing.
- Variety of approaches to learning, coupled with ‘state-of-the-art’ e-learning technologies.
- A pathway from Graduate Certificate to Graduate Diploma to Masters and PhD in cyber security and forensic computing.

- Opportunity to undertake intensive workshops in Adelaide.
- The program can be completed fully online by negotiation.
- The program is designed for professional development of IT practitioners within Australian Law Enforcement.
- Qualifications in both cyber security and forensic computing will enable graduates to meet the high demands in the Australian Defence and banking industries for professionally qualified IT Security Staff who have an undergraduate qualification in IT or engineering.
- Candidates will have strong interpersonal and excellent communication skills.

Program Features at a Glance

<table>
<thead>
<tr>
<th>Graduate Certificate in Science (Forensic Computing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graduate Certificate in Science (Cyber Security)</td>
</tr>
<tr>
<td>Graduate Diploma in Science (Cyber Security and Forensic Computing)</td>
</tr>
<tr>
<td>Master of Science (Cyber Security and Forensic Computing)</td>
</tr>
<tr>
<td>A pathway to a PhD in the areas of Cyber Security and Forensic Computing</td>
</tr>
</tbody>
</table>
Program Details

Graduate Certificate in Science (Forensic Computing)

<table>
<thead>
<tr>
<th>Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Evidence 1 – Forensic Computing</td>
</tr>
<tr>
<td>Electronic Evidence 2 – Network and Internet Forensics</td>
</tr>
<tr>
<td>Electronic Evidence Analysis and Presentation</td>
</tr>
<tr>
<td>E-Crime, E-Discovery and Forensic Readiness</td>
</tr>
</tbody>
</table>

Electronic Evidence 1 - Forensic Computing
To provide students with a sound knowledge and understanding to enable them to recover admissible evidence from PC based computers and the skills and competencies to prepare such evidence for presentation in a Court of Law and to develop knowledge and understanding of advanced forensic computing techniques and to acquire the skills to apply these successfully.

Electronic Evidence 2 - Network and Internet Forensics
To enable students to develop knowledge, understanding and skills for the recovery of admissible evidence from computers which are connected to a network and for the recovery of admissible evidence from computers which have been used to exchange data across the Internet.

E-Crime, E-Discovery and Forensic Readiness
To develop knowledge and understanding of the strategies, techniques and technologies used in the investigation of crime involving computers, devices, the Internet and associated networks and with a sound understanding of the practical aspects involved in preparing, presenting and explaining computer-derived evidence in non-computer literate courtrooms.

Electronic Evidence Analysis and Presentation
To provide students with a sound knowledge and understanding to enable them to apply NIST and ISO 17025 lab standards for validation and verification to a forensic computing lab, to comprehend continuity and exhibit management systems and documentation systems, to understand key legal aspects of computer crime and to provide expert evidence to the court.

Note: Upon successful completion of the Graduate Certificate (Forensic Computing) students can apply for entry to the Graduate Diploma and enrol in the remaining four courses.

Courses will consist of a mix of asynchronous online modules, student assignments, synchronous online interaction and face-to-face (synchronous) interaction during intensive teaching classes in Adelaide. While the proportions of these activities might vary from course to course, we are mindful of the need to ensure that the courses are offered in as flexible a manner as possible.
Graduate Certificate in Science (Cyber Security)

Intrusion Analysis and Response
To develop knowledge and understanding of the strategies, techniques and technologies used in attacking and defending networks and how to design secure networks and protect against intrusion, malware and other hacker exploits.

Critical Infrastructure and Control System Security
To understand the key policy issues and technologies underlying critical control infrastructures in various industries and the design considerations for these systems in light of threats of natural or man-made catastrophic events with a view to securing such critical systems.

Information Assurance and Security
To provide students with a deep understanding of the technical, management and organisational aspects of Information Assurance within a holistic legal and social framework.

Software Security Lifecycle
To provide students with a deep understanding of, and the ability to implement and manage security throughout the software development lifecycle.

Note: Upon successful completion of the Graduate Certificate (Cyber Security) students can apply for entry to the Graduate Diploma and enrol in the remaining four courses.
### Graduate Diploma in Science (Cyber Security and Forensic Computing)

<table>
<thead>
<tr>
<th>Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Evidence 1 – Forensic Computing</td>
</tr>
<tr>
<td>Electronic Evidence 2 – Network and Internet Forensics</td>
</tr>
<tr>
<td>Electronic Evidence Analysis and Presentation</td>
</tr>
<tr>
<td>e-Crime, e-Discovery and Forensic Readiness</td>
</tr>
<tr>
<td>Intrusion Analysis and Response</td>
</tr>
<tr>
<td>Critical Infrastructure and Control Systems Security</td>
</tr>
<tr>
<td>Information Assurance and Security</td>
</tr>
<tr>
<td>Software Security Lifecycle*</td>
</tr>
</tbody>
</table>

### Master of Science (Cyber Security and Forensic Computing)

<table>
<thead>
<tr>
<th>Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Evidence 1 – Forensic Computing</td>
</tr>
<tr>
<td>Electronic Evidence 2 – Network and Internet Forensics</td>
</tr>
<tr>
<td>Electronic Evidence Analysis and Presentation</td>
</tr>
<tr>
<td>e-Crime, e-Discovery and Forensic Readiness</td>
</tr>
<tr>
<td>Intrusion Analysis and Response</td>
</tr>
<tr>
<td>Critical Infrastructure and Control Systems Security</td>
</tr>
<tr>
<td>Information Assurance and Security</td>
</tr>
<tr>
<td>Software Security Lifecycle*</td>
</tr>
<tr>
<td>Masters Computing Minor Thesis 1</td>
</tr>
<tr>
<td>Masters Computing Minor Thesis 2</td>
</tr>
</tbody>
</table>

### CIS Research Methods

The research process; the content of research proposals in the IT/IS domain; writing a research proposal; research methodologies appropriate across the fields of Information Technology/Information Systems (IT/IS); investigating emerging issues in IT/IS; research frameworks for IT/IS; qualitative and quantitative research in IT/IS; appropriate use of statistical data analysis in IT/IS research projects; research software tools and their use.

### Masters Computing Minor Thesis 1 & 2

To develop the student’s ability to carry out a substantial Computer and Information Science research and development project under supervision, and to present results both at a research seminar and in the form of written documentation.

---

Students commencing with the Graduate Diploma must complete all eight courses.

Students commencing with the Masters Program must complete all ten courses.

*Note: Students must choose to take either Software Security Lifecycle or CIS Research Methods and should seek approval for their choice from the Program Director.
The program has a higher degree of structure in terms of the sequence of courses that must be undertaken, however, there is still some flexibility to accommodate students who wish to proceed through the program at different speeds.

Program Structure

Synchronous face-to-face during intensive week teaching in class
Allow 15 hours

Synchronous, in class (internal students) and online (external students) activity i.e. live, online staff-student interaction (lectures, tutorials, guest lectures, discussions, etc)
Allow not less than 12 hours

Asynchronous, self-paced and largely independent online learning
Allow up to 50 hours

Asynchronous and Synchronous interaction between staff-student and student-student. Virtual meetings, Assessment activities (assignments, projects etc.)
Allow 75-80 hours

To undertake the program students need as a minimum, the following:

Internet Explorer
Email
Adobe Acrobat Reader
Other tools to be advised e.g. Flash Player

Headphones/Microphone
Internet connection - preferably broadband
Microsoft Office (Word, Excel, PowerPoint)
International fees
International students at UniSA are required to pay international student fees. These fees are due and payable twice a year in $AUS and the amount varies depending on the program of study. International students studying in Australia must study full-time as stated in Australian Government regulations. Fees cover the full cost of tuition. They do not cover accommodation, books, living costs or Overseas Student Health Cover (OSHC) charges.

International students studying offshore can undertake their study part-time or full-time, and pay fees according to the study load they are enrolled in. For more information, please visit unisa.edu.au/international/fees

English Language
All courses for the program are taught in English and therefore it is essential for international students who speak English as a second language to show English language competency.

Entry requirement is
• International English Language Testing System (IELTS Academic), with a minimum score of 6.0 in Reading and Writing sub scores and minimum overall score of 7.0 (or equivalent) obtained with the last two years; or
• Successful completion of at least two years of tertiary study at diploma level or above conducted and completed in English within the last five years in a country in which English is an official language; or English is commonly used. Where study in English was more than five years ago, this requirement may be satisfied by subsequent and recent work experience of at least two years duration in a setting where English is the language of business, subject to satisfactory evidence as determined by the University.

For students who do not meet these requirements, English proficiency can be improved by study at the Centre for English Language (CELUSA) (unisa.edu.au/celusa). CELUSA provides a range of academic and general English programs and specialises in preparing students for study in Australia.

International Contact for Advice
For information please email international.office@unisa.edu.au
**Government Assistance**

This program is Commonwealth Supported and some domestic students may be eligible to defer their student contribution for all or part of their fees through the Australian Government Higher Education Loans program (HECS-HELP) and repay it through the taxation system. For more information, please visit goingtouni.gov.au

**Graduate Certificate**

Applicants are required to have a completed Bachelor Degree in a relevant discipline, science, engineering, technology, or a completed degree in any discipline plus three years work experience as a Forensic Computing, Information Assurance or Electronic Evidence professional; or a minimum of six years relevant professional experience in cyber security, forensic computing work experience in Law Enforcement, Defence or the commercial sector.

**Graduate Diploma**

Applicants are required to have a completed undergraduate degree from a recognised University in science, engineering or technology; OR a completed undergraduate degree in any discipline from a recognised University plus three years work experience as a Forensic Computing, Cyber Security or Electronic Evidence professional; OR a completed Graduate Certificate in Science (Forensic Computing) or Graduate Certificate in Science (Cyber Security) with an average of at least Pass Level 1 (55%), or equivalent.

**Master**

Applicants are required to have a completed undergraduate degree from a recognised University in science, engineering or technology with an average of at least credit (65%); OR a completed Graduate Diploma in Science (Cyber Security and Forensic Computing), with an average of at least credit (65%) or equivalent.

In addition, applicants for the Graduate Diploma and Masters would normally have passed coursework with the following contents:

- Computer programming
- Data modelling and database design
- Project Management
If you hold qualifications from another international university or institution, please refer to the Credit Transfer Register at unisa.edu.au/international/credit or contact the International Student Office at international.office@unisa.edu.au

All Applicants
For further information please contact Moira Lawler on 08 8302 6955 or email moira.lawler@unisa.edu.au

Submitting an Application
You will also be required to submit to the addresses shown:
- Certified copy of any degrees, diplomas, certificates or official transcripts from other institutions, and translations if not in English (Note: if you have previously studied at UniSA, you do not need to submit your UniSA transcripts).
- Certified copies of English language test results if applicable.
- An up to date detailed curriculum vitae outlining your experience as a Forensic Computing, Cyber Security or Electronic Evidence professional.

Australian Applications
If you are an Australian citizen living in Australia application for entry to this program is to be submitted via SATAC www.satac.edu.au

International Applications
If you are an international student, application for entry to this program is made via UniSA’s international office: www.unisa.edu.au/international/apply

Applications and Further Information
All documents must be in English and any translations must be accompanied by the documents in their original language. Only certified copies of any official documentation, such as transcripts, will be accepted. E-mailed or faxed copies will not be accepted.
The required documentation in support of your online application must be sent to:
UniSA International Office
University of South Australia
GPO Box 2471
Adelaide
South Australia 5001
Australia

Application Closing Dates
This program has two scheduled intakes per year.

- Study Period 2 (commences in March)
- Study Period 5 (commences in July)

The scheduled closing date for applications is one calendar month prior to the commencement of the Program.

Applications submitted after that time will be considered solely at the discretion of the Program Director.

Professional Recognition
The Graduate Diploma and Master programs have been granted accreditation for a period of 5 years by the Australian Computer Society.

This program is also supported nationally by all state law enforcement agencies, the private sector in Adelaide and nationally, Australian Federal Police and ISC2, an international not-for-profit information systems security and software lifecycle security certification body.

Students studying the program will develop relevant skills that will prepare them for the following professional certifications:

- Certified Information Systems Security Professional (CISSP) and
- Certified Security Software Lifecycle Professional (CSSLP)
“This course work has been developed as a direct result of the ongoing collaboration between the South Australia Police and the University of South Australia. Practitioners and educators have met to discuss and identify the skills that are required now to reduce and prevent the compromise of computers and associated devices.

The subjects and their content are of direct relevance to those who seek to understand the nature of threats in our increasingly technology enabled world. The learning outcomes provide students with skills in the area of forensic readiness, computer forensics, information assurance and the provision of expert evidence for court.”

Barry Blundell
Detective Senior Sergeant
Electronic Crime Section
South Australia Police
Glossary

Asynchronous
Asynchronous refers to activities in the LMIA program that do not take place in real time. Learning modules that students can access and study at any time, at their own pace are examples of asynchronous activities. Online discussion boards, where participants post messages for others to see and comment on, is another example of an asynchronous activity.

The LMIA Program
The Master of Science (Cyber Security and Forensic Computing) program offers three levels of enrolment: Graduate Certificate, Graduate Diploma and Masters. Entry to the program requires that students meet specified University entry requirements. This normally includes the completion of a four-year engineering or IT degree or six or more years of work experience in a relevant industry.

Graduate Certificate
A Graduate Certificate is a formal University award that requires completion of 18 units of study (normally four courses) at postgraduate level.

Graduate Diploma
A Graduate Diploma is a formal University award that requires completion of 36 units of study (normally eight courses) at postgraduate level.

Masters
A Masters Degree is a formal University award that requires completion of 54 units of study (normally twelve courses, or equivalent) at postgraduate level.

Course
A course is a collection of teaching and learning activities, including readings, lecture materials, assignments and discussion, which together address a related topic. In the flexible, blended (hybrid) learning environment of the LMIA program, a course consists of a number of asynchronous modules, various synchronous, online activities, and a synchronous, face-to-face, intensive teaching week in class. Together these activities develop the relevant knowledge and skills in students.

Learning Management System
This is a computerised system that acts as the focal point for flexible, online learning. Typically such a system provides students with a web interface, through which the student can access asynchronous learning modules, chat-rooms, virtual classrooms, discussion boards and the like. Good Learning Management Systems also provide administrative functions, such as a course calendar, that help students to track their progress, plan various study activities and communicate with staff and other students. The LMIA program will make use of Moodle – probably the world's de facto standard for Learning Management Systems.

Module
A module is a sub-unit of a course. In the LMIA program, a large proportion of the content of the program is delivered through asynchronous modules. Modules capture smaller, discrete topics in more manageable chunks. Together, these modules build into courses.

Synchronous
Synchronous refers to activities in the LMIA program that take place in real time, whether face-to-face, or online. The key characteristic is the “live” nature of the activity.
“Participation in the UniSA Information Assurance* program is fantastic from a range of perspectives. I have a lot of practical experience in forensic computer analysis, and completing the Graduate Certificate in Science (Forensic Computing) really helped to merge my theoretical understanding with my practical experience. The involvement of industry mentors in the program has ensured the subject matter is relevant and up to date with current forensic and security practice and knowledge. This, combined with the skills and knowledge of the lecturers, has provided a holistic understanding of the subjects. The Cyber Security subjects also involve industry experts, and the assignments are designed to provide a real world focus, in conjunction with current knowledge and research. Involvement in the program has enabled me to gain a deeper understanding of the theory and practical aspects of cyber security, forensic analysis and research.”

Darren Quick
Senior Consultant
stratsec.net | A BAE Systems Company

“I decided to undertake the Information Assurance* program at UniSA because I wanted to extend my knowledge in computer forensics and enhance my professional standing by obtaining a postgraduate qualification in my field. I chose UniSA because it had a broad range of courses, flexible study options and they had an established research focus in computer forensics. Undertaking this program has given me a different perspective of computer forensics and how it fits and overlaps with other cyber security and information assurance disciplines. So far I have found the courses to be highly practical and relevant to my work, and I have gained exposure to other closely related fields including IT security and intrusion analysis. Each course has a weekly virtual seminar component which is great for those studying by distance as it provides a forum to interact with other students and the lecturer in real-time. Coupled with the opportunity to meet and learn from other industry experts during the intensive week, there is a lot of added value to the course.”

Syd Pleno
Senior Computer Forensic Examiner
Australian Federal Police

* Cyber Security and Forensic Computing was formerly Information Assurance
Dr Elena Sitnikova is a professional researcher and academic with a career which includes over fifteen years of engineering experience in the space and IT industry. Elena has a wide knowledge of communication control systems, software and systems engineering. Current research interests are in the areas of critical infrastructure protection and security, quality assurance and enterprise process capability improvement.

Prior to joining UniSA Elena worked for five years at the Motorola Australia Global Software Group where she successfully aligned a broad range of expertise in project management, process and quality management, and all phases of the complete software development life cycle. Elena is also interested in research in the area of engineering education.

Elena is one of the first Certified Security Software Lifecycle Professionals (CSSLP) in Australia. She is among the first group of eleven women that have graduated from the Australian Women in IT and Science Entity’s South Australian Board Readiness Program.

Before migrating to Australia in 1998, Elena worked in Tbilisi, Georgia. The results of her research in the area of mathematical modelling and optimal control were applied to the BURAN (Snow Storm) shuttle program which was implemented at the Research and Production Association ENERGIA, Moscow, Russia (known as the Russian Space Research Centre).

**Awards and Prizes**

- **2008** - UniSA Enhancing Learning Award (Category: Services Supporting Student Learning) within the Mawson International Transitions Team for applying a new approach in teaching Postgraduate masters courses that supports international students, in particular, in their transitions to new academic ways.

- **2005** - for achievements in developing and coordinating professional courses was awarded the Employee of the year 2005 from the Systems Engineering and Evaluation Centre (SEEC) at UniSA.

- **2002** - for contribution as a training instructor to the success of the Motorola Technical Training Program was awarded the Certificate of Appreciation.
Ask UniSA

Australian Students
Moira Lawler
Telephone: 08 8302 6955
Email: moira.lawler@unisa.edu.au

International Students
For information specific, please contact
Telephone +61 3 96274854
Web: unisa.edu.au/international
Email: international.office@unisa.edu.au

To view the program website, go to
cis.unisa.edu.au

While every effort is made to provide full and accurate information at the time of publication, the University does not give any warranties in relation to the accuracy and completeness of the contents.

The University also reserves the right to discontinue or vary arrangements programs, courses (units), assessment requirements and admission requirements without prior notice.