Institutional Catalog: 2014

The SANS Technology Institute (“STI”) institutional catalog is published to help familiarize potential and current students with the resources available to assist them in the pursuit of their educational goals. It is a reference including information about academic requirements, STI policies, student rights and responsibilities, and methods for accessing important services.

Information contained in the catalog is current as of the date of publication. We have made every effort in the preparation of the catalog to provide pertinent and accurate information. Periodically, we revise policies and procedures after publishing the catalog. Significant changes concerning new academic regulations, policies or programs will be published on our website (www.sans.edu) and an email will be sent to all students. We recommend students periodically visit the website to review the most up-to-date information.

For current students, if you find a section you do not understand or would like a statement clarified, please contact the Office of Student Advising, advising@sans.edu, or contact your academic program’s director:

- For the MSISE program: Dr. Eric Cole ecole@sans.edu
- For the MSISM program: Dr. Jim Voorhees jvoorhees@sans.edu

Again, welcome to SANS Technology Institute.

Regards,

Toby Gouker, Ph.D
Provost
tgouker@sans.edu
## Table of Contents

Academic Integrity, Network and Responsible Computing Policy .............................................................. 7
Mission ....................................................................................................................................................... 8
Vision .......................................................................................................................................................... 8
Institutional Goals ..................................................................................................................................... 8
Accreditation and Approvals ...................................................................................................................... 8
Federal Education Rights and Privacy Act (FERPA) .................................................................................. 9
Affiliations .................................................................................................................................................. 9
Governance, Faculty and Administration ................................................................................................. 10
   Board of Directors .................................................................................................................................. 10
   Faculty ..................................................................................................................................................... 11
      Program Faculty ................................................................................................................................... 11
   Administrators ....................................................................................................................................... 12
   Staff Directory ...................................................................................................................................... 13
Academic Calendar ....................................................................................................................................... 13
   2014 Learning Event Schedule .............................................................................................................. 13
Admissions Requirements ........................................................................................................................ 14
   Notice to International Students ........................................................................................................... 14
Student Identification Policy ..................................................................................................................... 15
Tuition .......................................................................................................................................................... 15
Fees .............................................................................................................................................................. 16
   Financial Aid / Scholarships .................................................................................................................. 16
   Paying Tuition and Registering for Courses ......................................................................................... 16
   Refund and Change Fees ...................................................................................................................... 16
Academic Policies ........................................................................................................................................ 17
   Academic Freedom ............................................................................................................................... 17
   Intellectual Property Rights .................................................................................................................. 17
   Transfer Credit Policy ........................................................................................................................... 17
   Waivers of Courses or Course Requirements ....................................................................................... 18
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Institute Classes within SANS Technology Institute Courses</td>
<td>18</td>
</tr>
<tr>
<td>GIAC Certifications</td>
<td>18</td>
</tr>
<tr>
<td>GIAC Gold Papers</td>
<td>18</td>
</tr>
<tr>
<td>PMP Certification</td>
<td>19</td>
</tr>
<tr>
<td>CISSP Certification</td>
<td>19</td>
</tr>
<tr>
<td>CISA Certification</td>
<td>19</td>
</tr>
<tr>
<td>Withdrawal Policy</td>
<td>19</td>
</tr>
<tr>
<td>Leave of Absence Policy</td>
<td>19</td>
</tr>
<tr>
<td>Dismissal from Institute</td>
<td>19</td>
</tr>
<tr>
<td>Appeal of Dismissal</td>
<td>21</td>
</tr>
<tr>
<td>Satisfactory Academic Progress</td>
<td>22</td>
</tr>
<tr>
<td>SAP Appeal Process</td>
<td>23</td>
</tr>
<tr>
<td>Reapplication to SANS Technology Institute</td>
<td>24</td>
</tr>
<tr>
<td>Grading</td>
<td>25</td>
</tr>
<tr>
<td>Attendance</td>
<td>25</td>
</tr>
<tr>
<td>Grading System</td>
<td>25</td>
</tr>
<tr>
<td>Notice regarding GIAC Proctored Exams</td>
<td>26</td>
</tr>
<tr>
<td>Student Services</td>
<td>28</td>
</tr>
<tr>
<td>Disability Accommodations in Academic Programs</td>
<td>28</td>
</tr>
<tr>
<td>Transcripts</td>
<td>28</td>
</tr>
<tr>
<td>Communication with other Students</td>
<td>28</td>
</tr>
<tr>
<td>Student Organizations</td>
<td>28</td>
</tr>
<tr>
<td>Student ID Card With Photo</td>
<td>28</td>
</tr>
<tr>
<td>Sans.edu Email Address</td>
<td>29</td>
</tr>
<tr>
<td>Change of Personal Information</td>
<td>29</td>
</tr>
<tr>
<td>Institutional Code of Conduct</td>
<td>29</td>
</tr>
<tr>
<td>Non-Discrimination and Anti-Harassment</td>
<td>30</td>
</tr>
<tr>
<td>Academic Conduct</td>
<td>30</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>31</td>
</tr>
<tr>
<td>Weapons Policy</td>
<td>31</td>
</tr>
<tr>
<td>Visitors and Children at STI Events</td>
<td>31</td>
</tr>
</tbody>
</table>
Grievances ........................................................................................................................................... 31
Educational Resources .......................................................................................................................... 32
Facilities ............................................................................................................................................... 32
SANS Learning Resource Center .......................................................................................................... 32
  Borrowing Book Resources .................................................................................................................. 33
  Internet Storm Center/DShield Resources .......................................................................................... 34
  Other Resources on STI’s Website ........................................................................................................ 34
  General IT and Management Resources ............................................................................................. 34
  Case Study and Research Databases ................................................................................................... 34
  Magazine Databases ............................................................................................................................ 35
Programs of Study .................................................................................................................................. 36
Master of Science Degrees .................................................................................................................... 36
Application Requirements and Process .................................................................................................. 36
Master of Science in Information Security Engineering ........................................................................ 40
  MSISE Program Learning Outcomes .................................................................................................. 41
  MSISE Graduation Requirements ........................................................................................................ 41
Master of Science in Information Security Management ...................................................................... 42
  MSISM Program Learning Outcomes ................................................................................................ 42
  MSISM Graduation Requirements ....................................................................................................... 43
Post-baccalaureate Certificate Programs ............................................................................................ 44
Application Requirements and Process ............................................................................................... 44
Cybersecurity Engineering Core ........................................................................................................... 47
  Program Learning Outcomes ................................................................................................................ 47
  Cybersecurity Engineering Core Graduation Requirements .................................................................. 47
Penetration Testing & Ethical Hacking ..................................................................................................... 48
  Program Learning Outcomes ................................................................................................................ 48
  Penetration Testing & Ethical Hacking Graduation Requirements ....................................................... 49
Incident Response ................................................................................................................................ 49
  Program Learning Outcomes ................................................................................................................. 49
  Incident Response Graduation Requirements ....................................................................................... 50
Course Listings and Descriptions ........................................................................................................... 51
Academic Integrity, Network and Responsible Computing Policy

Integrity in teaching and learning is a fundamental principle of a graduate school. All members of our Institute’s community share the responsibility for academic integrity. Faculty members are expected to establish classroom environments conducive to the maintenance of academic integrity, provide students a syllabus describing the course and its requirements, and grade submitted work promptly and adequately. Students are expected to conduct themselves in a manner that will contribute to maintaining academic integrity.

Academic dishonesty is the failure to maintain academic integrity. Academic dishonesty includes, but is not limited to: cheating; fabrication; bribery offered for grades, transcripts, or diplomas; obtaining or giving aid on an examination; having unauthorized prior knowledge of an examination; doing work for another student; presenting another student's work as one's own; and plagiarism.

Plagiarism is the presentation of another person's idea(s) or product(s) as one's own without acknowledging their source(s) or receiving appropriate permission(s) to use the idea or product.

Students can avoid unintentional plagiarism by carefully following accepted scholarly practices. Notes taken for papers and research projects should accurately record sources of material to be cited, quoted, paraphrased, or summarized, and papers should acknowledge these sources in references. A first act of plagiarism may result in an automatic reduction in the student's grade. Multiple acts of plagiarism shall result in dismissal from the program.

All course examinations are open book, and proctored exams are usually required.

When you take an ethical hacking or penetration testing course, you will be asked to sign the following before you are granted access to computing and network resources related to that class:

I certify that by having access to tools and programs that can be used to break or “hack” into systems, that I will only use them in an ethical, professional and legal manner. This means that I will only use them to test the current strength of security networks so that proper improvements can be made. I will always get permission before running any of these tools on a network. If for some reason I do not use these tools in a proper manner, I do not hold SANS or the presenter liable and accept full responsibility for my actions.

Name__________________________ Signature__________________________

Company_______________________ Date_____________________________
Mission

The SANS Technology Institute develops leaders to strengthen enterprise and global information security. STI educates managers and engineers in information security practices and techniques, attracts top scholar-practitioners as faculty, and engages both students and faculty in real-world applied research.

Vision

The SANS Technology Institute aspires to be the preeminent graduate institution translating contemporary information security practice and scholarship into effective educational experiences. Our graduates will be highly valued because they design state-of-the-art, enterprise-level cyber defenses, champion the adoption of those defenses, and manage their implementation and ongoing operation.

Institutional Goals

In so doing, STI will:

1. Enable private and public sector enterprises of the United States and its allies to preserve social order and protect their economic rights and military capabilities in the face of cyber attacks;
2. Provide the national defense establishment, critical industries, businesses and government agencies with information security engineers and managers who have the most current and critical knowledge and skills needed to respond effectively to the evolving cyber attack landscape; and,
3. Perform leading-edge research that continually identifies current best practice and enhances the state of the art in the practice of information security.

Accreditation and Authorization

The SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education (3624 Market Street, Philadelphia, PA 19104 - 267.284.5000) an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

SANS Technology Institute is authorized by the Maryland Higher Education Commission to offer Master of Science degrees in Information Security Engineering and Information Security Management, and Post-baccalaureate Certificates in Cybersecurity Engineering Core, Incident Response, and Penetration Testing and Ethical Hacking.
Federal Education Rights and Privacy Act (FERPA)

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

An an eligible student, you would have the right to inspect and review your own education records.

STI requires written permission from the eligible student in order to release any information from a student's education record. However, FERPA allows STI to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

Information on FERPA can be found at the U.S. Department of Education webpage: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Affiliations

STI is an independent, wholly-owned subsidiary of the Escal Institute for Advanced Technologies, dba The SANS Institute, the premier global provider of information security training. STI is also affiliated with GIAC, another subsidiary of the SANS Institute responsible for testing and certifications in the information security field.
Governance, Faculty and Administration

Board of Directors
STI is governed by an independent Board of Directors that plays an active role in guiding the college, from helping to shape the mission, goals, and Strategic Plan to actively reviewing assessment data and helping to identify solutions to difficult challenges. Members of the Board represent varying constituencies and bring wide-ranging perspectives to their service in helping STI achieve its mission and goals. Directors serve a three-year term and are eligible for re-election. The STI Board members are listed below:

- Mason Brown, Chairman, is the CEO of the SANS Institute, our parent organization. He also brings to the Board the perspective of a business leader, having served as chief operating officer of a division of Alcoa. He is a respected force in cybersecurity, having been selected to represent the business community’s perspective on the Commission on Cybersecurity for the 44th Presidency.

- Dennis Kirby, Vice Chair, is a member of the SANS management team primarily responsible for training content and instructor development. After graduating from the U.S. Military Academy, he was Commander of a UH-60 Blackhawk Assault Helicopter Company of the 101st Airborne Division and served in Desert Storm. A graduate of Harvard Business School, he has managed private equity investments exceeding $1 billion and served on multiple boards of directors of portfolio companies.

- Dr. Ron Phipps is a senior associate at the Institute for Higher Education Policy, where he co-authored Assuring Quality in Distance Education: A Preliminary Review for the Council for Higher Education Accreditation. He previously served as Assistant Secretary at the Maryland Higher Education Commission and as Executive Director of the Alaska Commission on Postsecondary Education.

- Dr. Thomas Johnson is Associate Vice President and Chief of Strategic Initiatives at Webster University. Dr. Johnson previously served as Dean of the College of Criminal Justice and Forensic Sciences at the University of New Haven for 13 years, during which time he worked with faculty to develop new programs in the areas of national security, digital forensics, and advanced investigation.

- Scott Cassity is the Managing Director of the Global Information Assurance Certification (GIAC) organization, and as such he bolsters the Board’s insight into student testing, certification, and evaluations. Mr. Cassity was previously an executive in a healthcare, real estate development, and consulting firm, and he is the current President of ChildHelp of East Tennessee, a children’s advocacy organization.

- Richard Hammer is the Information System Security Officer (ISSO) for the Advanced Nuclear Technology group (N-2) at Los Alamos National Laboratory. He was the first graduate of STI.

- Lenny Zeltzer earned his MBA from the Sloan School at MIT and is now a Product Management Director at NCR Corporation, where he focuses on safeguarding IT infrastructure of small and mid-size businesses around the world. He also teaches digital forensics and malware courses for the SANS Institute, where he is a senior faculty member.
• Dave Shackleford is a consultant and author in cybersecurity. He previously served as Chief Security Officer for Configuresoft and as Chief Technology Officer for the Center for Internet Security. He is the author of *Virtualization Security: Protecting Virtualized Environments*, and recently coauthored the first course on virtualization security for the SANS Institute. He helps lead the Atlanta chapter of the Cloud Security Alliance.

• Ed Skoudis is the founder of Counter Hack Challenges, an innovative organization that designs, builds, and operates popular information security challenges and simulators including CyberCity, NetWars, Cyber Quests, and *Cyber Foundations*. His expertise includes hacker attacks and defenses, and he has trained more cyber penetration testers than anyone else in America. He is the author of two Prentice Hall best sellers, *Counter Hack Reloaded* and *Malware: Fighting Malicious Code*.

• STI President Alan Paller and Rick Wanner, Manager in Corporate Security at SaskTel and a current student at STI, serve as nonvoting members.

Faculty

The faculty is the primary reason that a SANS Technology Institute educational experience allows students to become technical leaders in information security in their organizations. At SANS Technology Institute, you learn security from people who are the top experts in the field, the authors of the most authoritative books, and, most importantly, from people who have front-line, in-the-trenches experience doing the types of jobs that you will be required to do. Each member of the SANS faculty has demonstrated himself or herself to be highly competent, on the basis of formal education and professional experience, to provide educational courses that meet the objectives laid out in the program goals.

Program Faculty

Program faculty serve as the primary authors and instructors for STI courses, and they are directly involved in the design and maintenance of current and future courses, program design and student learning outcomes.

Dr. Johannes Ullrich, Ph.D. Physics, SUNY Albany
Dr. Eric Cole, DPS, Computing, Pace University
Stephen Northcutt, Bachelor of Science, Mary Washington College
Ed Skoudis, M.S., Information Networking, Carnegie Mellon University
Lenny Zeltser, M.B.A. from M.I.T.
Dave Shackleford, M.B.A, Georgia State University
Rob Lee, M.B.A. Georgetown University
Jeff Frisk, Bachelor of Science, Engineering, Rochester Institute of Technology
David Hoelzer, Bachelor of Science, Information Technology
Administrators

Administrators for SANS Technology Institute provide leadership to carry out plans and activities in support of the college's goals and objectives. STI administrators create and design appropriate processes and services to support students and the learning environment.

Alan Paller
President

Toby Gouker, Ph.D.
Provost; Chief Academic Officer

Eric Cole, DPS
MSISE Program Director

James Voorhees, Ph.D.
MSISM Program Director

David Hoelzer
Dean of Faculty

Johannes Ullrich, Ph.D.
Director of Research

Stephen Northcutt
Past President
Dean of Student Advising

William Lockhart
Executive Director

Matthew Scott
Director, Institutional Effectiveness

Shelley Moore
Assistant Director, Student Enrollment and Communications

Diane Sardi
Registrar
Staff Directory

Students are welcome to contact STI Staff and Faculty with questions or comments.
  - For topics related to enrollment, please contact Shelley Moore via admissions@sans.edu or Diane Sardi via registrar@sans.edu.
  - For topics related to Academic Advising, please contact Stephen Northcutt, Dean of Student Advising (snorthcutt@sans.edu) or Toby Gouker, Ph.D. (tgouker@sans.edu), Provost/Chief Academic Officer.
  - For topics related to research or papers, in addition to the relevant faculty members for the course, please contact Johannes Ullrich, Ph.D, Dean of Research (jullrich@sans.edu).
  - Alan Paller (apaller@sans.edu) is our President.

Academic Calendar

STI operates on a continuous enrollment basis and class instruction may be taken in a live classroom or via one of several distributed learning environments, as available. Given our open enrollment model we operate one academic term per year that starts January 1 and ends on December 31. Applications are accepted throughout the year.

Office hours are Monday through Friday, 8:00 a.m. to 5:00 p.m (EST). The Institute’s offices are closed on: New Year’s Day, Memorial Day, Independence Day, Labor Day, Thanksgiving and the Friday after Thanksgiving, and Christmas.

Graduation is held in the fall or winter of each year in conjunction with the SANS Network Security or SANS Cyber Defense learning events.

2014 Learning Event Schedule

<table>
<thead>
<tr>
<th>Event</th>
<th>Hotel/Location</th>
<th>City</th>
<th>State</th>
<th>Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Quarter 2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SANS Security East 2014</td>
<td>Sheraton New Orleans</td>
<td>New Orleans</td>
<td>LA</td>
<td>1/18/14</td>
</tr>
<tr>
<td>SANS Scottsdale 2014</td>
<td>Hilton Scottsdale</td>
<td>Scottsdale</td>
<td>AZ</td>
<td>2/15/14</td>
</tr>
<tr>
<td>SANS Monterey 2014</td>
<td>Marriott Monterey</td>
<td>Monterey</td>
<td>CA</td>
<td>3/2/2014</td>
</tr>
<tr>
<td>SANS Cyber Guardian 2014</td>
<td>Sheraton Inner Harbor</td>
<td>Inner Harbor</td>
<td>MD</td>
<td>3/2/14</td>
</tr>
<tr>
<td>SANS Northern Virginia 2014</td>
<td>Sheraton Reston</td>
<td>Reston</td>
<td>VA</td>
<td>3/16/14</td>
</tr>
</tbody>
</table>

2nd Quarter 2014
Admissions Requirements

All Applicants, regardless of program, must meet the following criteria:

- Have at least 12 months of professional work experience in information technology, security or audit.
- Be employed or have current access to an organizational environment that allows them to apply the concepts and hands-on technical skills learned in their program of study.
- Have earned a baccalaureate degree from a recognized college or university, or equivalent international education, with a minimum cumulative grade point average of 2.8.

Notice to International Students

We welcome students from all over the world. Although based in Maryland, the SANS Technology Institute's programs will serve students in all states and many countries around the world. Although students do not need to reside in the US to complete the program, STI is not involved with securing educational or travel visas for international students. Please be prepared to make the necessary accommodations before applying to the Institute. When presenting a non-US transcript for admissions, candidates must first have their transcripts...
evaluated by World Education Services [http://www.wes.org/students/index.asp](http://www.wes.org/students/index.asp) before completing their submission to STI.

While STI runs an international program, all courseware is delivered in the English language. The Test of English as a Foreign Language (TOEFL) is, therefore, required for applicants whose native language is not English. We require a minimum score requirement of 100 (Internet-based test) over-all with each of the sub-categories (Reading, Listening, Speaking, Writing) achieving a minimum of 25 each. The test scores must be sent to us directly by the testing agency. The TOEFL Bulletin of Information and registration form can be obtained at American embassies and consulates, offices of the United States Information Service (USIS) and U.S. education commissions.

Applicants who cannot obtain a TOEFL Bulletin and registration form locally may request them from:

TOEFL/TSE Services  
P.O. Box 6151  
Princeton, NJ 08541-6151 USA  
1-609-771-7100 or 1-877-3546 or 1-609-771-7714

**Student Identification Policy**

STI’s policy on verifying student identity can be downloaded at: [https://www.sans.edu/downloads/policy-regarding-verification-of-student-identity.pdf](https://www.sans.edu/downloads/policy-regarding-verification-of-student-identity.pdf).

You will require a photo ID at any SANS event in order to access your facilities pass and materials.

STI operates a distributed learning environment where many courses are available on-line. In order to maintain the academic integrity of the Institute students will be required to provide proof of identification throughout their program of study. Students can only access on-line course by logging into their portal account using established credentials. All exams at STI are proctored (See notice on GIAC exams). Students schedule exams through the GIAC site, using established log-on credentials. At the exam site, students must show two (2) forms of personal ID. Both must have your signature and both must be current. One of the two must have your photo. The ID bearing both your signature and photo must be government-issued. Students access the exam by logging into their portal account, using established credentials.

**Tuition**

The cost per credit hour is $1250 in both the MSISE and MSISM Program.

Each program requires 36 credits (36 x $1,250 = $45,000). The Program Capstone will cost $2,098.

Students are responsible for the costs of hotel, food and travel to attend any of the residential institutes. The average hotel and food cost, if the hotel rooms are not shared, is $1,200 per residential institute,
though significant savings are available through room sharing. These amounts are to be paid directly to the hotel at which the residential institute is being conducted.

Fees

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Fee*</td>
<td>$100</td>
</tr>
<tr>
<td>Late Course Change Fee</td>
<td>$250</td>
</tr>
</tbody>
</table>

* Paid during application process

Financial Aid / Scholarships

At the present time, SANS Technology Institute does not administer scholarships or other federal financial aid programs. STI recommends student’s check with their employers regarding tuition reimbursement or assistance programs for which they may be eligible.

Paying Tuition and Registering for Courses

STI students are required to pay STI's established tuition at the time of registration for each course. Discounts or promotions offered by SANS Institute (an affiliate of STI) for individual course elements will not apply. STI students will utilize STI’s course registration page provided in new student orientation materials.

Refund and Change Fees

SANS Technology Institute students who wish to cancel and receive a refund for a particular graduate course, or element within or portion of a graduate course, whether or not they are also withdrawing from the program, must submit a cancel/change/refund request by email to registrar@sans.edu by the earlier of a) 30 days prior to the start of the course or b) whatever date is associated with the refund policy of SANS or GIAC relative to the particular course element for which a student is seeking a refund, as found on the www.sans.org or www.giac.org websites. For purposes of this refund policy, the start date of the course shall be considered: a) for graduate courses that include a SANS Institute class, either the first day of the associated SANS Residential Institute for which the student was registered or, for courses delivered via our OnDemand platform, the first day when the student has access to the course materials in their SANS portal account, or b) for other graduate courses not requiring a SANS Institute class or GIAC certification, the start date shall be 30 days prior to the date requiring the participation and/or interaction of faculty, SANS academic staff or Gold advisors.

In the event that a SANS Technology Institute student seeks to change the venue, timing, or modality for a particular element within a graduate course, they may do so free of charge if they submit their change request to
registrar@sans.edu prior to the date associated with a refund for that same course or element. However, if they submit a change request after the associated refund date, their request will be subject to a $250 late fee. This is the same procedure that would apply to a student who wishes to change their choice of electives. Please note that withdrawing from a course without re-scheduling that course may affect your academic standing.

STI may choose to participate in programs that allow US armed forces service members to utilize tuition assistance subject to the Department of Defense’s Voluntary Education Partnership’s Memorandum of Understanding: Students participating in this program may, in accordance with the terms of that Memorandum of Understanding, receive a refund for a course up to and including the day prior to the start of the course without incurring any change or late fees. Refunds of government-funded tuition assistance in this program will go to the applicable Service and not to the Service member.

Academic Policies

Academic Freedom

Academic freedom is essential to the advancement of knowledge and understanding, and transmission of this knowledge to others. STI supports and encourages freedom of inquiry for both faculty and students so they may responsibly pursue these goals through teaching, learning, research, discussion, and publication, free from both internal and external restraints that would unreasonably restrict their academic pursuits.

Intellectual Property Rights

In accordance with copyright law, all faculty-directed student writing assignments, including answer material for tests, projects, research papers and business plans prepared in connection with any course, are the property of SANS Technology Institute and may be used by the Institute for any educational purposes it deems appropriate.

Transfer Credit Policy

The SANS Technology Institute does not generally accept transfers of credit for coursework completed at other higher education institutions. Any decision to make an exception to this policy in a given individual instance would need to be approved by the Curriculum, Academic, Faculty, and Student Affairs Committee, after prior approval by the appropriate Program Director or the Provost.

The SANS Technology Institute does in certain circumstances waive requirements for course elements or courses within its program of studies as a reflection of a student's previous attainment of substantially similar intended learning outcomes. Waivers may be granted for up to, but not more than, one-quarter of the total number of credit hours or credit-hour equivalents required by the program, and are subject to various limits, requirements, and fees as described below. Waivers will not be granted when the requirements of the waiver are met after a student matriculates, regardless of any alternative arrangements or costs available to take such
course elements outside of the our program and fee structure. In the event a waiver is granted for an entire course, no credit hours or grade will be awarded, nor will the course figure into the calculation of a student's cumulative grade point average. In the event a waiver is granted for part of a course’s components, the grade(s) received on the remaining components completed by the matriculated student will be used to determine the course grade, and full-course credit hours will be awarded.

**Waivers of Courses or Course Requirements**

**SANS Institute Classes within SANS Technology Institute Courses**

The SANS Technology Institute will grant a waiver to a student from the requirement within a SANS Technology Institute course to complete a specific SANS Institute class when the student has completed that class within the two years prior to matriculation, subject to the requirement that the student completes any remaining SANS Technology Institute course requirements associated with that course after matriculation but prior to taking additional courses. For example, a student who completed the SANS Institute class SEC 401 precisely two years prior to matriculation must, upon matriculation, complete the associated GIAC GSEC exam and Gold Paper required by ISE 5100 prior to enrolling in additional courses within the program.

**GIAC Certifications**

The SANS Technology Institute will grant a waiver to a student from the requirements within a course to complete both a relevant SANS Institute class and GIAC exam if the student has taken and passed the relevant GIAC exam within the past three years. Waivers for GIAC certifications achieved without having taken the relevant SANS Institute class (“GIAC Challenges”) will be subject to, and contribute to, the existing limit of two GIAC Challenges allowed. Similar to above, a student receiving such a waiver must complete any required associated Gold Papers prior to proceeding with additional courses within the program. For example, an MSISE student who within the past three years has taken the GIAC GSEC exam will be granted a waiver from the requirements of ISE 5100 from having to retake the SANS Institute's SEC 401 class and GIAC GSEC exam but, nevertheless, in this instance, such a student would still be required to complete and pass the required GSEC Gold Paper requirement in order to receive credit for ISE 5100.

**GIAC Gold Papers**

In the event a student prior to matriculation has successfully completed a GIAC Gold Paper required by a course in the program, the requirements of the entire course associated with said GIAC Gold Paper will be waived, subject to the requirement that a) the GIAC Gold Paper shall have been completed within the five years prior to the student's matriculation date, and b) that the student has both taken or renewed the associated GIAC exam within the prior three years. Waivers for entire courses where the GIAC certification was achieved without having taken the relevant SANS course (“GIAC Challenges”) will be subject to, and contribute to, the existing limit of two GIAC Challenges allowed, regardless of the score achieved.
PMP Certification
For students who hold a current PMP from the Project Management Institute, a waiver will be granted for the requirement to take ISE/ISM 5800 in its entirety (waiving both the component SANS MGT 525 course and the GIAC GCPM requirement).

CISSP Certification
For students who hold a current CISSP from the ISC2 organization, a waiver will be granted within ISE/ISM 5100 for the SANS Institute class SEC 401 or MGT 512, respectively. Achievement of the associated GIAC GSEC or GSLC certifications, respectively, and completion of the associated Gold Paper for either course will still be required for the award of credit.

CISA Certification
For students who hold a current CISA from the ISACA, a waiver will be granted for the SANS AUD 507 and GIAC GSNA exam course components of ISM 6200. However, the student with such waiver is still required to complete the Gold/Written assignment prior to the award of credit.

Students who have received a waiver but still must complete either or both an associated GIAC exam or Gold Paper, will be charged for these additional experiences in accordance with the tuition and fees in place at the time the student seeks to engage in these activities for credit.

Withdrawal Policy
If you choose to withdraw from the Institute you must notify registrar@sans.edu in writing as soon as is reasonably possible. After the request has been received, your student records will be updated to reflect the date of your withdrawal. Please see the refund policy for refunds on tuition payments made.

Leave of Absence Policy
The SANS Technology Institute (“STI”) expects its students to maintain continuous registration in an academic program. However, it is sometimes necessary or desirable for a student to take a leave from enrollment for a period of time, for purposes of national service, serious illness, or material personal or financial difficulties. The determination of “material” will be the sole responsibility of the SANS Technology Institute.

Students seeking to take a leave of absence must first contact the Dean of Academic Affairs, or their appointed Academic Advisor, to discuss the need for a Leave of Absence and their plans to return to active status. A student taking a leave of absence must declare a firm, and time-bounded intention to return by a certain date. A leave of absence requested while a student is enrolled in a class activity does not qualify the student for any refund of tuition for the class in progress. Please see refund policy on tuition payments.
A formal letter must be written and sent to the Provoist by all students requesting a leave of absence. Notifying instructors or no longer attending/working on classes does not initiate or complete the process. A leave of absence may be requested for national service, serious illness, or for personal or financial reasons. After completion of the letter, you must email it to the Provost for approval. Before approving the request, the Provost may call or write to you to request more information.

STI is committed to handling reasonable requests for leaves in a responsible manner. This policy may not be used in lieu of disciplinary action to address any violations of institute rules, regulations, policies, or practices. A student who is granted a voluntary leave while on academic and/or disciplinary status will return to that same status upon return to the institute.

Students on leave are not permitted to attend SANS or STI classes or take GIAC or STI exams while their leave is in effect. A student who is granted a leave of absence will still be required to complete all degree requirements; however, regarding the requirement to complete their program requirements within the specified time of enrollment, a leave will extend the specific time period for completing the program by the length of the approved leave of absence.

Except where a leave is mandated by compulsory national service, the duration of the leave generally will be a maximum of twelve (12) months. An extension or reduction of the leave period may be granted for good cause.

Leaves will take effect as of the date signed by the Provost. After the Leave of Absence is received by the registrar, it will be reviewed for grade implications.

**Procedures:**

1. The student should discuss a leave of absence with his or her academic advisor.
2. The student must write a “Leave of Absence Letter” and provide supporting documentation. The “Leave of Absence Letter” is submitted to the Provost.
3. If the student is seeking a leave due to a medical or psychological condition, STI may require the student to submit evidence of the applicable condition from his or her health provider.
4. The student will be notified in writing by Provost of the approval or denial of the request for a leave. If the request is approved, the terms and conditions of the leave shall be set forth in the approval notification.
5. The Provost will be responsible for notifying the appropriate University offices, administrators, faculty advisors, and instructors of the approval of the leave.
6. If a leave is approved, the student’s access to and use of her/his e-mail account will continue, unless the Provost decides otherwise. The student may visit Institute functions only with the written permission of the Provost. Such permission will be set forth in the letter approving the leave.
7. The notation “leave of absence” and applicable dates will be entered on the student’s transcript.

**Return from a Leave of Absence/Re-enrollment:**
1. On/about six (6) weeks prior to the first day of class for which you seek to return, you must notify the Provost via email, of your intention to return or re-enroll at the conclusion of the leave period.
2. If the voluntary leave was due to a psychological or medical condition, and STI had required evidence from your health provider, you must satisfy the Provost with regards to your fitness to re-enroll, including the submission of additional evidence from your health provider.
3. A student who fails to register for classes within two (2) months from the end of their Leave of Absence will be dismissed from the program and would need to apply for readmission.

Dismissal from Institute

Students will be subject to dismissal procedures for the following reasons:

(1) Not making satisfactory academic progress (see Satisfactory Academic Progress policy below)
(2) Engaging in Illegal/Unacceptable Behavior

Engaging in illegal or other unacceptable behavior as described in this catalog will subject students to dismissal from the Institute. STI will notify the student of the accusation, and the student will be given a reasonable time to respond in writing to the accusation. After reviewing the accusation and the response, STI will render a decision regarding the violation(s). In some cases, it will be deemed to merit a dismissal. If so, STI will notify the student of the dismissal, the effective date of the dismissal, and that the student has 30 days to appeal the dismissal.

Notice to Students Regarding Dismissal

In the field of information security, email communication is the standard method of notice. Notices to students will be sent to the student's email address. If it is clear to STI that the student is no longer at that email address, then STI will send the notice by certified mail from an STI administrator.

- If it is possible for the student to correct the situation, then he/she will be given a statement about what must be done within a certain time to resolve the problem. If the student does not meet the requirements within that time, then he/she can be dismissed from the degree program; in which case the student will be given notification of the dismissal. That notice will state when the effective date of the dismissal, and that the student has 30 days to appeal the dismissal.
- If the situation is not subject to correction, the student will be notified of the dismissal, the effective date of the dismissal will be effective, and that the student has 30 days to appeal the dismissal.

Please see the refund policy for refunds on tuition payments made.

Appeal of Dismissal
Students may appeal their dismissal within 30 days of the notice of dismissal that is provided by STI to the student. The student should send a notice to the Dean of Academic Affairs. The Provost will review the appeal and make a binding decision within 30 days.

**Satisfactory Academic Progress**

When you make the decision to pursue a degree, you make a substantial commitment of time and financial resources. In return, STI encourages and assists you in completing your academic goals in a timely manner to allow you to utilize your newly acquired capabilities outside the academic environment as soon as possible. This policy applies to all students enrolled at STI.

Students must maintain at least a cumulative 3.0 official grade point average (GPA). GPA is calculated by dividing the grade points earned by the number of credits attempted. Only STI courses are used in the calculation, and “pass-fail” courses are not included.

Along with an acceptable GPA, you must complete your program within five years, and maintain Satisfactory Academic Progress. Conditions and processes defined in this policy were developed to align with federal education guidelines for satisfactory academic progress: US Department of Education regulation 34 CFR §668.34.

At STI, Satisfactory Academic Progress (SAP) requires earning a minimum of 8 credit hours per year.

Students will be placed on SAP probation if their pace of study falls below an average of 8 credits hours earned per year. If a student’s pace of study falls below an average of 6 credit hours per year, they will be subject to dismissal from the Institute. Calculation of SAP will be conducted annually based upon the date of a student’s admission into the program.

**Examples:**

<table>
<thead>
<tr>
<th>Cumulative Earned Hours</th>
<th>Years in Program</th>
<th>SAP Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>3</td>
<td>12/3 = 4; Does NOT meet SAP</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>12/1 = 12; Does MEET SAP</td>
</tr>
<tr>
<td>12 plus 8 waived</td>
<td>3</td>
<td>12/3 = 4; Does NOT meet SAP</td>
</tr>
</tbody>
</table>

Students must also be on target to complete their academic program while maintaining a successful level of course completions. To determine if a student is meeting this standard, total cumulative earned hours are compared to total cumulative attempted hours. “Attempted Hours” include the sum of hours associated with each failed or successfully completed course. For example, a student who first fails a course and then passes it...
would have “6 attempted hours” and “3 earned hours.” Students must successfully complete at least 2/3 of the credit hours attempted within a year in order to be considered as making satisfactory academic progress.

Examples:

<table>
<thead>
<tr>
<th>Cumulative Earned Hours</th>
<th>Cumulative Attempted Hours</th>
<th>SAP Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>24</td>
<td>$12/24 = 50%$; Does NOT meet SAP</td>
</tr>
<tr>
<td>12</td>
<td>15</td>
<td>$12/15=80%$; Does MEET SAP</td>
</tr>
</tbody>
</table>

If a student does not meet SAP standards, they will be placed on probation and notified at the email address on file with STI within 10 days. Students then have one term to either earn the GPA or semester hours required to meet the minimum requirements, or submit an SAP appeal. Failure to complete the two steps above will result in dismissal procedures. It is the responsibility of every student to monitor their academic progress and to be aware of the requirements of their program and the SAP standards.

**SAP Appeal Process**

An SAP appeal is considered if the student can demonstrate:

- Failure to meet the minimum standard was caused by extreme or unusual circumstances beyond their control, and;
- They have resolved the issue(s) that caused the deficit, and;
- The issue(s) will not affect their performance in the future.
- If an appeal is approved, the student’s probation will be temporarily suspended pending review at the end of the next term the student is enrolled. If at that time the standards are not being met, probationary status will be reinstated.

When a student corrects their challenge of not meeting the SAP standards, the student will be removed from SAP probation.

**Instructions to the Student for Submitting an Appeal**

1. Write an appeal that explains:
   - Failure to meet the minimum standard was caused by extreme or unusual circumstances beyond their control, and;
   - They have resolved the issue(s) that caused the deficit, and;
   - How the issue(s) will not affect their performance in the future.

2. Attach any pertinent supporting documentation.
Documentation of circumstances described in your letter must be included with the written appeal. Note: the inability to attend classes due to lack of funds is not an extenuating circumstance. Refer to the list below for required documentation. Additional documentation may be requested after your appeal is reviewed.

3. Submit the appeal application, letter, and documentation to the enrollment management office. Retain a copy of all documents submitted for your records. No documents will be returned.

The Provost/Chief Academic Officer will review your appeal. All decisions are final. You will receive written notification of the decision made on your appeal. A second review may only be requested if you can provide new information and documentation that may have been omitted from the initial appeal.

Reapplication to SANS Technology Institute

Applicants applying for re-admission to SANS Technology Institute's Masters Degree Program must submit the following:

- The application form described above. Please write "Application for Re-Admission" and "I have NOT consulted or corresponded with any SANS faculty/instructor or staff member regarding re-admission" OR "I have consulted or corresponded with [insert name], who is a SANS faculty/instructor or staff member regarding re-admission" at the top.
- Reapplication Fee
- Current Resume with Three References
- Employer Letter of Recommendation

Applicants are not required to provide additional supplemental materials (transcripts, test scores) unless their original application is over two years old.
Grading

Attendance
Students are expected to attend all course sessions. If you are unable to attend a course session, please contact your academic advisor with as much advance notice as possible. Please submit any documentation necessary with your notice. It is up to the instructor’s discretion to allow students to make-up any missed assignments or submit assignments late. We encourage students to review the course syllabi for specific attendance and assignment requirements as well as important course deadlines. Failure to maintain regular course participation (meeting substantial course deadlines every 30 days) may result in students being withdrawn from the course without a refund of tuition.

Student participation includes student-to-faculty, student-to-student and student-to-community interaction. Class interactivity contributes to overall student learning and a feeling of connectedness.

Grading System
Grades represent the faculty’s evaluation of student competencies in a course. Grades assigned by SANS Technology Institute faculty are derived from a variety of assessment instruments administered by the faculty and/or third party evaluators, such as the GIAC organization. Each course’s syllabus contains specifics on the components of a course that are used by the faculty to formulate a grade for the course. At the completion of each course, grades are calculated by the faculty and reported to the Office of the Registrar. Grades are recorded in the student’s digital academic record.

Procedures:
1. The course faculty is responsible for ensuring that each course syllabus contains specifics on the components of a course that are used by the faculty to formulate a grade for the course.
2. Students should feel free to ask for an explanation of the grading practices in any course.
3. At the completion of work in a course, faculty will assign one of the following grades:

<table>
<thead>
<tr>
<th>Letter</th>
<th>Grade Points (per credit hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>4.0</td>
</tr>
<tr>
<td>A-</td>
<td>3.7</td>
</tr>
<tr>
<td>B+</td>
<td>3.3</td>
</tr>
<tr>
<td>B</td>
<td>3.0</td>
</tr>
<tr>
<td>B-</td>
<td>2.7</td>
</tr>
<tr>
<td>C+</td>
<td>2.3</td>
</tr>
<tr>
<td>C</td>
<td>2.0</td>
</tr>
<tr>
<td>F</td>
<td>0.0</td>
</tr>
</tbody>
</table>
4. If the student fails to complete all of the required course parts before the allotted time for the course expires, faculty will enter a provisional grade of “I” (Incomplete) for the course. The student will then have 30 days to complete the remaining course parts so that the faculty can replace the grade of “I” with the appropriate letter grade. If the student does not complete the remaining course parts within the 30 day period, the Office of the Registrar will replace the grade of “I” with a grade of “F” for the course, unless the faculty member responsible for the course grants an exception.

5. A grade assigned for work in a course is not subject to change except in the case of a specific error, which may be corrected upon the request of the faculty for the course, in writing, to the Registrar not later than one month after the completion of the course.

Questions concerning this policy or its intent should be directed to the Office of the Registrar.

Notice regarding GIAC Proctored Exams

STI uses the services of the GIAC organization for many of the exams given in STI courses. In addition to benchmarking a student’s classwork knowledge acquisition against industry job standards, students will also earn an industry-leading certification as a result of their successful study.

The following is an excerpt from the GIAC website that describes the exam taking experience and requirements:

One Exam Format

All GIAC certification attempts are comprised of a single exam that will cover all certification objectives. Certification exams are 2-5 hours in length, depending on the specific certification attempt. For details on individual certifications, go to http://www.giac.org/certifications/categories

Open Book Policy

GIAC certification exams are open book format, but not open internet or open computer. Candidates are allowed to bring “one armful” of books and notes into the testing room, leaving all other personal belongings outside of the testing room. An erasable note board and pen will be provided for you. Workstation space is limited, so please plan accordingly. No electronic devices are allowed such as extra computers, CD-ROM, USB flash drives, phones, calculators, cameras, etc. Candidates will not be able to access anything stored electronically on any computer during the exam such as searchable .pdf or Word documents. We recommend that you print any study guide materials and bring them as hard, paper copies.

Finding a Proctor for your GIAC Certification Exam

The primary method for taking a proctored exam is through GIAC’s testing partner, Pearson VUE. Pearson VUE is an industry leader and offers more than 3,500 testing centers worldwide. It is expected that any
candidate within a reasonable driving distance (1-2 hours) from a Pearson VUE testing center will utilize this option. Visit www.giac.org/testing centers to locate the closest Pearson VUE testing center.

If you will be taking a GIAC proctored exam in the future and do not see a testing center within a reasonable driving distance (1-2 hours), please email proctor@giac.org. Do not attempt to schedule a testing appointment with Pearson VUE before you have registered for a GIAC certification and have received access to your certification attempt through your portal account.

The scheduling process for Pearson VUE will be web-based through your SANS/GIAC portal account. The specific steps for scheduling a proctored exam through Pearson VUE can be viewed at: How to Schedule Your GIAC Proctored Exam. Exam slots are available on a first come, first serve basis. You should schedule your appointment at least one month before you wish to take your exam.

Should you need to cancel or reschedule your scheduled exam appointment, you must do so at least one business day (24 hours) prior to your exam appointment by logging into your SANS/GIAC account and clicking on 'Certification Attempts,' 'View Proctor Details' and then 'Change.' If you need to cancel or reschedule your exam less than 24 hours in advance, you will forfeit your appointment and be charged a $150 seating fee. To reschedule, log into your SANS account and click on 'Certification Attempts,' 'View Proctor Details' and then 'Reschedule.' To cancel, call our customer service line at 301-654-7267.)

Be prepared to show two (2) forms of personal ID. Both must have your signature and both must be current. One of the two must have your photo. The ID bearing both your signature and photo must be government-issued.

If you have questions regarding scheduling your proctored exam, please email proctor@giac.org or call 301-654-7267.
Student Services

Disability Accommodations in Academic Programs

Applicants and prospective or current students with disabilities who require academic adjustments and/or auxiliary aids throughout the admissions process, and/or throughout their studies should contact the enrollment management office for assistance. It is the student’s responsibility to request accommodations and to provide current and supporting documentation explaining the nature and limitations of their disability. The STI faculty and staff will work with the student to make reasonable accommodations and adjustments to enable them to fully participate in the admissions process and educational programs.

Transcripts

Academic records are maintained for every student that has enrolled at STI, and transcripts are available upon request. In accordance with the Family Rights & Privacy Act (FERPA) records cannot be released without a student's written consent. Students have the right to review records maintained by STI and request information they believe to be inaccurate or misleading be removed from their records. STI will utilize the grievance process described under grievances to resolve issues with academic records. Students/alumni may request transcripts of their STI records by emailing registrar@sans.edu or writing to SANS Technology Institute at 8120 Woodmont Avenue, Suite 310, Bethesda, MD 20814.

Communication with other Students

Contacting other STI students can be an excellent way to work on projects, share knowledge and generally assist each other. If you would like to join the STI email list, send your request to info@sans.edu.

Student Organizations

To promote the organization and networking of students, there is a student email list so that students can communicate with other students. There is also a SANS Technology Institute group on LinkedIn.

Student ID Card With Photo

If you would like to have a photo ID card showing that you are a student of STI, email the following to info@sans.edu:

-- Your photo (headshot, no hats, basically in the nature of a passport type photo).
-- The mailing address where the ID card should be mailed
The card may be helpful in obtaining discounts from some manufacturers/suppliers who offer such discounts. Also, some university/college libraries may allow STI students to have library privileges if they show a student ID card with a photo.

**Sans.edu Email Address**

An “@mastersprogram.sans.edu” email address may be helpful in obtaining discounts from some manufacturers/suppliers who offer such discounts. The format we use is as follows: [first initial][lastname]@mastersprogram.sans.edu If you are interested in having an “@mastersprogram.sans.edu” email alias address, please make this request to: registrar@sans.edu. In the request, designate the email address to which this “@mastersprogram.sans.edu” address should be forwarded.

**Change of Personal Information**

To change your personal information, log into your SANS portal account, then click on personal information. You can update all common information such as physical address and email address, work and home phone numbers, job titles, etc. You are responsible for keeping your personal information up to date in order to receive important communications from STI in a timely manner.

**Institutional Code of Conduct**

The purpose of this code of conduct is to express STI’s expectations for conduct and to identify behaviors outside of the acceptable bounds of behavior. We ask students and faculty members to become familiar with and govern themselves by this code of conduct.

Mature behavior and conduct consistent with the highest professional standards of the information security community are expected of every student while attending a residential educational event, other live educational events, or engaging in Institute-related online activities. STI reserves the right to place on probation, or dismiss, students who engage in unsatisfactory conduct such as disorderly behavior, failure to adhere to rules and regulations, failure to exhibit proper online etiquette, destruction or theft of property, participation in activity that impinges on the rights of others, or the excessive consumption of alcoholic beverages or use of any illegal drugs at any time while participating in an STI sponsored activity.

As educated adults who are leaders and advisors to organizations on compliance with laws and regulations, students are held to a high standard in terms of both knowledge and the application of trust, law and regulation. Violations of city, state, and federal laws while enrolled at STI may also constitute violations of the code of conduct. In such instances, the Institute may proceed with disciplinary action under the code, independent of any criminal proceeding involving the same conduct, and may impose sanctions for violation of the code even if such criminal proceeding has not been resolved or is resolved in the student's favor.
Non-Discrimination and Anti-Harassment

STI is committed to maintaining an environment of appropriate conduct among all persons and respect for individual values. The Institute is committed to enforcing non-discrimination and anti-harassment in order to create an environment free from discrimination, harassment, retaliation and/or sexual assault. Discrimination or harassment based on race, gender and/or gender identity or expression, color, creed, religion, age, national origin, ethnicity, disability, veteran or military status, sex, sexual orientation, pregnancy, genetic information, marital status, citizenship status, or on any other legally prohibited basis is unlawful and undermines the character and purpose of STI. Such discrimination or harassment will not be tolerated.

The Provost is charged with investigating allegations of discrimination and harassment in the working and learning environments. Please write tgouker@sans.edu if you have a concern.

Academic Conduct

STI’s expects all students to engage in their activities in a fashion consistent with the very highest standards of academic integrity.

Examples of academic misconduct include, but are not limited to:

• Subverting the examination process, exchanging, transmitting, or receiving information during examinations, the possession and/or use of unauthorized materials during those examinations, or providing or enlisting assistance for a student taking examinations.
• Submitting plagiarized work for any assignment. Students should be aware that STI uses Turnitin and other services to detect plagiarism.
• Dishonest or falsified reporting of research results.
• Engaging in activities that unfairly place other students at a disadvantage, such as taking, hiding or altering resource material, or manipulating a grading system.
• Misuse of hacking, malicious code, information warfare or other techniques. In general, the difference between a hacker and a system administrator is permission.

Any action(s) reported or observed by a student, faculty or staff member in violation of the SANS Technology Institute's Code of Conduct policy will be reported to the provost, president or the appropriate staff. A staff member will notify the accused in writing of the violation(s) and the individual will be afforded an opportunity to respond in writing to the accusation. After reviewing the accusation and the response, the appropriate STI staff members will render a decision regarding the violation(s). An appeal may be made to the president of SANS Technology Institute and he will review the staff's decision. The president’s decision will be final.

http://www.sans.edu/students/codes-of-conduct
Safety and Security

Students are expected to take reasonable actions in the areas of health and safety. Prohibited or discouraged conducts include:

- Attending group functions when you are suffering from a serious infectious disease that may be transmitted.
- Ignoring obvious safety hazards such as blocked exits or accumulation of flammables.
- Knowingly reporting a false emergency.
- Any action that puts another person’s safety, physical or mental health, or life at risk, whether intentionally or as a result of recklessness or negligence.

Weapons Policy

All members of the STI community, including faculty, staff, students and visitors are prohibited from possessing, discharging, or otherwise using “weapons” on premises where STI functions are taking place whether or not the person has been issued a federal or state license to possess such weapons. Any person violating this policy will be subject to disciplinary action including but not limited to suspension, expulsion, termination, removal from Institute premises or events and/or criminal prosecution. Exceptions to this policy are considered on an individual basis and only in consideration of the student’s employment.

A weapon is defined as:

- Any device that shoots a bullet, pellet, flare or any other projectile, whether loaded or unloaded, including those powered by CO2. This includes but is not limited to rifles, shotguns, handguns or other firearm, BB/pellet gun, flare gun, stun gun or dart gun and any ammunition for any such device. Any replica of the foregoing is also prohibited.
- Any explosive device including firecrackers and black powder.
- Any device that is designed or traditionally used to inflict harm including but not limited to any knife with a blade longer than three inches, hunting knife, fixed blade knife, throwing knives, dagger, razor or other cutting instrument the blade of which is exposed.

Visitors and Children at STI Events

Visitors and children are welcome at graduation and the vendor shows at STI Residential Institutes; however, they may not accompany STI students to classrooms, events or student-only events such as STI roundtables.

Grievances

Appeal procedures regarding academic matters are described in the academic policies section. Specific processes have been established for grades, academic probation and dismissal. If a student has completed the
appeals process and would like to make a formal grievance regarding the decision, process, or file a grievance regarding a violation of the institutional code of conduct, they may do so by contacting the Provost by email providing reasonable details regarding their grievance with appropriate evidence to support their claims. The Provost will review the grievance and take appropriate steps to reconcile the matter. The student will receive an email response within 30 days.

Educational Resources

Facilities

STI does not operate a traditional brick and mortar campus. In person class instruction is conducted through learning events hosted at hotel venues and other facilities across the United States and in select foreign countries.

SANS Learning Resource Center

The challenges of information security are constantly evolving, and excellence in performance demands continuous monitoring of changes in threats, technology, and practices. SANS conducts an extensive research program that will help STI students and alumni maintain their edge in security. All of these services are available at no cost to STI students and alumni unless otherwise specified. SANS supplies a learning resource center through the SANS Resources Center, which is a compilation of thousands of original research papers, security policies, security notes, along with a wealth of unique network security data.

1. SANS Information Security Reading Room contains nearly 2,000 original research studies, not available from any other source, in over 70 categories relevant to the study of information security. The papers in the SANS Reading Room are prepared by information security professionals to meet the requirements to earn GIAC (Global Information Assurance Certification) certifications. On average, each of the papers reflects 60 to 90 hours of original research.

2. The SANS Security Policy Collection contains model security policies developed by major corporations and government agencies. They serve as guides and templates for security managers who need to understand and create effective security policies. At the time this was written, the Policy collection contained approximately 35 policies. The collection grows as new security issues arise and policy templates are needed.

3. The SANS 20 Critical Controls is a consensus list of vulnerabilities that require immediate remediation. It is the result of a process that brought together dozens of leading security experts. They come from the most security-conscious government agencies in the UK, US, and Singapore; the leading security software vendors and consulting firms; the top university-based security programs; the Internet Storm Center, and many other user organizations.
4. The SANS Newsletter Collection helps you to keep up with the high level perspective of the latest security news.

5. The Security Glossary is among the largest glossary of security terms available on the Internet, it was developed jointly by SANS and the National Security Agency. It provides authoritative definitions of many of the specialized terms students will encounter.

6. The SANS Collection of Frequently Asked Questions about Intrusion Detection contains 118 authoritative discussions of the primary topics that arise when planning and implementing intrusion detection technologies.

7. The SANS Internet Storm Center Archives contains contemporaneous analyses of new attacks that are discovered on the Internet. Internet Storm Center is the first site most government and commercial security officers visit after learning of a new attack because experts come together at that site to share what they have learned about the damage being done by the new attack and what can be done to block the attack. The archives form an extraordinary research asset because of the depth of the analysis and the currency of the topics covered. Internet Storm Center archives also provide STI students with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects looking at attack patterns and how fast worms spread through the Internet.

8. S.C.O.R.E. A community of security professionals working to develop consensus regarding minimum standards and best practice information. This cooperative research program delivers authoritative checklists and tools that enable you to measure the effectiveness of the security of various aspects of your defensive arsenal.

9. SANS Web Briefings. Several times a month, STI and SANS faculty, and other Security experts provide up-to-date web briefings for STI alumni on new threats seen at Internet Storm Center, new technologies that are emerging, and analysis of security trends. These web briefings are archived so you may listen to them at any time.

10. Popular Resources on Computer Security FAQ providing answers to common information requests about computer security and links to additional reading.

11. SANS Resources Center constantly adds resource material, so please check it frequently.

12. The GIAC resources page offers several white papers on key issues included in the Common Body of Knowledge and is a rich source of resources for every person seeking certification and technical expertise in network security and information security.

Borrowing Book Resources
STI does not maintain an official library. However, we do maintain a list of books that may be borrowed from various faculty and staff members. To view the list of these books, click on the Excel spreadsheet here. Students may have up to 3 borrowed books in their possession at the same time for research on papers and projects that are required by the Master's Program. Students may keep the book(s) for up to one month and may renew the book(s) for one additional month by sending an e-mail request to info@sans.edu before the original due date. Requests for a book(s) should be e-mailed to info@sans.edu. If the book is available, it will be mailed to the student by first class mail or priority mail or similar method to the address that the student indicates. Students must return them in good condition using first class mail or priority mail or similar method with a postmark on or earlier than the due date. (Students should NOT use a "book rate" mailing method of return since it is too slow). If a student loses a book, they must pay for the cost of replacement (including tax and shipping cost, if any) plus a $15.00 handling charge.

**Internet Storm Center/DShield Resources**

Internet Storm Center/DShield - (DShield/ISC) data will be available for use by master's degree students of STI as follows: The student must submit a one page proposal to jullrich@sans.org outlining how the student wishes to use it. If the request is approved, the student will be given ssh access to the DShield data via its research mirror at the University of Wisconsin, or the student will be given a VPN account to access the malware lab.

**Other Resources on STI’s Website**

The resources section of STI’s website also includes current and graduate master's student's Presentations and Projects.

**General IT and Management Resources**

The following resources are available to STI students, and are maintained by other organizations. Many of the resources are freely available, but some require registration and fees for use:

**Case Study and Research Databases**

a. [Harvard Business School Working Knowledge](#) provides access to a wealth of research on management, finance, operations, negotiation and related management topics.

b. [INSEAD Knowledge](#) offers access to articles, case studies, working papers, and other material on innovation, finance, entrepreneurship, marketing, people leadership and more.

c. [Knowledge Wharton](#) has articles and case studies on managing technology, finance, ethics, and more.

d. [Harvard Business Online Case Study Library](#) is a rich collection of case studies covering many aspects of management.
Magazine Databases

a. MagPortal.com provides a search engine for locating individual magazine articles on the web.
b. Periodicals in Maryland Libraries provide a listing of periodicals owned by Maryland libraries — useful when unable to find the full text articles online.
c. FindArticles.com offers access to articles published in the last two years from over 300 publications.
Programs of Study

STI offers the following programs of study:

- Master of Science in Information Security Engineering
- Master of Science in Information Security Management
- Post-baccalaureate certificate: Cybersecurity Engineering Core
- Post-baccalaureate certificate: Incident Response
- Post-baccalaureate certificate: Penetration Testing & Ethical Hacking

Master of Science Degrees

Application Requirements and Process

All applicants must meet the following criteria:

- Have at least 12 months of professional work experience in information technology, security or audit.
- Be employed or have current access to an organizational environment that allows students to apply the concepts and hands-on technical skills learned in their program of study.
- Have earned a baccalaureate degree from a recognized college or university, or equivalent international education, with a minimum cumulative grade point average of 2.8.

Admissions Application Form and Application Fee

A nonrefundable application fee of $100.00 must be submitted with your application. The Application Fee must be paid via credit card, U.S. currency or check, international money order, or an international check in U.S. funds drawn on a bank in the United States.

Send checks to:

SANS Technology Institute
8120 Woodmont Ave., Suite 310
Bethesda, MD 20814

Or call 301-654-7267 with your credit card information, and explain that you are making payment for the admission fee of $100.
Applications will not be considered without payment of the application fee.

**Official Transcript(s)**

Please have your college/university submit official transcripts directly to:

SANS Technology Institute  
Attn: Master's Program - Applications  
PO Box 130957  
Dallas, TX 75313

For prospective students applying from outside of the United States:

Although based in Maryland, the SANS Technology Institute's programs serves students in all states and many countries around the world. When presenting a non-US transcript for admissions, candidates must first have their transcripts evaluated by World Education Services [http://www.wes.org/students/index.asp](http://www.wes.org/students/index.asp) before completing their submission to STI.

**Letter of Recommendation**

A letter of recommendation from your employer, or one of your customers if you are a consultant, will help the admissions committee evaluate your application. Applicant's employer must furnish a recommendation form supporting Applicant's continuing education. Please download the Employer Recommendation Request Form [online](http://www.sans.edu).

**Résumé**

Please send a current résumé that highlights your related work experience in information security.

**Outcome Statement**

This is an important step in the application process, so please give it your best effort.

If you are accepted to STI, you can expect to make a sizable investment in time, energy and money to complete the program. To protect you and to remain true to our mission statement, the admissions office asks you to complete an Outcome Statement as part of the admissions process. This step helps STI determine whether or not your goals and interests fit with ours.

**Purpose:**

- The purpose of the Outcome Statement is to tell us what you expect the outcome in your life to be after successfully completing your Master's Degree.
• It is preferable if you provide some details of your background and experience.
• We will review your Outcome Statement periodically to see if you are making progress toward achieving your desired outcome.

Requirements:

• Acceptable Outcome Statements are typically one to two typed pages.

Leadership Essay

Purpose:

STI seeks to admit students who have demonstrated leadership ability in the past and who will become the leaders in information security in the future. For that reason, we require all applicants to submit a leadership essay describing leadership qualities that the applicant has demonstrated in the past. We define leadership and leadership competencies in the article posted on our website. We are looking at the quality of the writing (content, grammar, spelling, etc.) since our master's program is writing intensive.

Requirements:

Your leadership essay will be comprised of two parts.

• Part A: List three competencies that you believe you have some strength in and provide examples. It is perfectly acceptable to refer to a competency that is not listed in the article referenced above.
• Part B: List three competencies that you want to work on. Please use a separate piece of paper for Part B.

Video Presentation

Purpose:

An important part of developing leaders to strengthen enterprise and global information security is ensuring the ability to communicate. The STI Master's programs are designed to improve both written and oral presentation communication skills while providing a strong, hands-on technical base to candidates. Your leadership essay and outcome statement provide us with a baseline on your written communications skills, and this 3-5 minute video presentation will baseline your oral presentation skills.

Requirements:

Please prepare and record a 3-5 minute video on any subject of your choosing. You can make a video presentation of your outcome statement or leadership essay, create a how-to video, describe a belief or opinion you hold, or tell us more about something of interest to you. The subject of the video, or its quality (please feel
free to use a phone or even your computer's webcam to execute the video), is less important than the video's role in enabling the admissions committee to sample your current presentation skills in a professional environment.

Slide presentations are neither required nor encouraged. When complete, please upload the video into Vimeo and submit the appropriate URL and password for viewing. Please see the Vimeo website for acceptable video recording parameters.

If English is not Applicant's Native Language:

- The Test of English as a Foreign Language (TOEFL) is required for Applicants whose native language is not English. We require a minimum score requirement of 100 (Internet-based test) over-all with each of the sub-categories (Reading, Listening, Speaking, Writing) preferred to be at a minimum of 25 each. The test scores must be sent to us directly by the testing agency. The TOEFL Bulletin of Information and registration form can be obtained at American embassies and consulates, offices of the United States Information Service (USIS) and U.S. education commissions.

Applicants who cannot obtain a TOEFL Bulletin and registration form locally, may request them from:

TOEFL/TSE Services
P.O. Box 6151
Princeton, NJ 08541-6151 USA
1-609-771-7100 or 1-877-3546 or 1-609-771-7714

TOEFL Web Site  http://www.toefl.com/

- IELTS can be used as a substitute for TOEFL. We require a minimum score requirement of 7.5 over-all with each of the sub-categories in IELTS preferred to be at a minimum of 7.5 each. IELTS scores must be sent to us directly by the testing agency.
- If you are a resident alien, please enclose a copy of your appropriate documentation with your application.

Application Submission

The completed Application for Admission and supporting credentials should be emailed to admissions@sans.edu, or if necessary, may be mailed to:

SANS Technology Institute
Attn: Master's Program - Applications
PO Box 130957
Dallas, TX 75313

We will notify you within five business days of receiving your complete application package.
• Application Packages will be reviewed by SANS Technology Institute’s Admissions Committee.
• All information and materials furnished may be verified to preserve the integrity of the Institute, and each Applicant may be scheduled for a prequalification telephone/online (or in-person if convenient) interview.

Invitation to Matriculate

Once the Admissions Committee reviews and approves your application for admission, the Enrollment Management office will send you an "Offer of Admission," requiring your signature and return. This "Offer of Admission" letter will be contingent on two additional elements:

• First, working in concert with the Provost or another student advisor, you must complete a Program of Study plan, noting in detail where and when you intend to take courses during the first twelve months of your program participation, and generally how you will complete the program in the subsequent years.
• Second, this planning conversation must also address the student's ability to fund his or her anticipated program of studies. The purpose of this conversation is to ensure the student recognizes the investment - both time and resources - required to complete the program. Once the applicant and Provost agree and sign off on an acceptable Program of Study plan, the applicant will return this signed Program of Study plan along with his or her counter-signed offer of admission, and will be formally matriculated into the master's program.

Course Requirement Waivers (Optional)

If the candidate is applying for a waiver of any course requirements, please indicate so on the Applicant Information Form.

Master of Science in Information Security Engineering

The program of study for the Master of Science in Information Security Engineering (MSISE) leads to proficiency in knowledge and skills that enable security practitioners to excel as technical leaders. The program is designed to ensure that each student achieves knowledge of the core, foundational domains of information security, plus allows them through elective choices to develop either concentrations in particular domains, or add to the breadth of their expertise by exploring a mixed set of topics beyond the core areas. The MSISE program prepares students to weave deep technical expertise into the design of effective cybersecurity. It also provides them with the communications skills and knowledge to gain proactive support for security enhancements from (1) higher-level management, (2) other peer organizational leaders and staff who must cooperate in adopting the enhancements, and (3) technical team members who must build and deploy those enhancements.
MSISE Program Learning Outcomes

By the end of this program, graduates will be able to:

- Formulate and implement policies and solutions that demonstrate a thorough understanding of security foundations and practical applications of information technology.
- Demonstrate a solid foundation in information security strategies and apply their knowledge by assessing an information security situation and prescribing an appropriate security approach.
- Construct an information security approach that balances organizational needs with those of confidentiality, integrity and availability. Solutions require a comprehensive approach that aligns with policy, technology, and organizational education, training and awareness programs.
- Effectively communicate information security assessments, plans and actions for technical and nontechnical audiences/stakeholders.
- Identify emerging information security issues, utilize knowledge of information security theory to investigate causes and solutions, and delineate strategies guided by evolving information security research and theory.
- Analyze and design technical information security controls and safeguards, including system specific policies, network, and platform security countermeasures and access controls.
- Conduct threat assessments (offensive measures), appraise/prioritize vulnerabilities (defensive perspectives), and appraise technical risks for enterprise information assets/needs/requirements.
- Apply a standards-based approach to minimize risk through the implementation of the principles and applications of information security.
- Evaluate the appropriate security solutions required to design/build a security architecture - this includes the integration of intrusion detection, defensive infrastructures, penetration testing, and vulnerability analysis.
- Formulate plans for adaptive detection of threats, including leading/oversight of intrusion/malware detection, incident response, forensics, reverse engineering, and e-discovery initiatives and actions.

MSISE Graduation Requirements

The MSISE program requires completion of 36 credit hours with a 3.0 G.P.A, within 5 years. Students must complete the following requirements:

<table>
<thead>
<tr>
<th>Required Course</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISE 5000 Research &amp; Communications Methods</td>
<td>0.5</td>
</tr>
<tr>
<td>ISE 5100 Enterprise Information Security</td>
<td>4</td>
</tr>
<tr>
<td>ISE 5200 Hacking Techniques &amp; Incident Response</td>
<td>4</td>
</tr>
<tr>
<td>ISE 5300 Building Security Awareness</td>
<td>1</td>
</tr>
<tr>
<td>ISE 5400 Advanced Network Intrusion Detection &amp; Analysis</td>
<td>4</td>
</tr>
</tbody>
</table>
### MSISM Program Learning Outcomes

By the end of this program, you will be able to:

- Formulate and implement policies and solutions that demonstrate a thorough understanding of security foundations and practical applications of information technology.
- Demonstrate a solid foundation in information security strategies and apply their knowledge by assessing an information security situation and prescribing an appropriate security approach.
- Construct an information security approach that balances organizational needs with those of confidentiality, integrity and availability. Solutions require a comprehensive approach that aligns with policy, technology, and organizational education, training and awareness programs.
- Effectively communicate information security assessments, plans and actions for technical and nontechnical audiences/stakeholders.
- Identify emerging information security issues, utilize knowledge of information security theory to investigate causes and solutions, and delineate strategies guided by evolving information security research and theory.

Apply a standards based approach to implement the principles and applications of risk management, including business impact analyses, cost-benefit analyses, and implementation methods that map to business needs/requirements.

Integrate the elements of information security management - Policy, Strategic and Continuity Planning, Programs and Personnel - into a coordinated operation.

Articulate positive and socially responsible positions on ethical and legal issues associated with the protection of information and privacy.

Devise incident response strategies, including business continuity planning/disaster recovery planning (BCP/DRP) initiatives, while focusing on cost effectiveness from both a proactive and reactive perspective.

**MSISM Graduation Requirements**

The MSISM program requires completion of 36 credit hours with a 3.0 G.P.A, within 5 years. Students must complete the following requirements:

<table>
<thead>
<tr>
<th>Required Course</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISM 5000 Research &amp; Communications Methods</td>
<td>0.5</td>
</tr>
<tr>
<td>ISM 5100 Enterprise Information Security</td>
<td>4</td>
</tr>
<tr>
<td>ISM 5200 Hacking Techniques &amp; Incident Response</td>
<td>4</td>
</tr>
<tr>
<td>ISM 5300 Building Security Awareness</td>
<td>1</td>
</tr>
<tr>
<td>ISM 5400 IT Security Planning, Policy and Leadership</td>
<td>3</td>
</tr>
<tr>
<td>ISM 5500 Research Presentation 1</td>
<td>1</td>
</tr>
<tr>
<td>ISM 5600 Legal Issues in Data Security and Investigations</td>
<td>4</td>
</tr>
<tr>
<td>ISM 5700 Incident Response Practicum</td>
<td>1</td>
</tr>
<tr>
<td>ISM 5800 IT Security Project Management</td>
<td>3</td>
</tr>
<tr>
<td>ISM 5900 Research Presentation 2</td>
<td>1</td>
</tr>
<tr>
<td>ISM 6000 Standards Based Implementation of Security</td>
<td>4</td>
</tr>
<tr>
<td>ISM 6100 Security Project Practicum</td>
<td>2</td>
</tr>
<tr>
<td>ISM 6200 Auditing Networks, Perimeters and Systems</td>
<td>4</td>
</tr>
<tr>
<td>ISM 6900 Information Security Fieldwork</td>
<td>0.5</td>
</tr>
<tr>
<td>Technical Elective (1 course)*</td>
<td>3</td>
</tr>
<tr>
<td>Required Program Capstone</td>
<td>0</td>
</tr>
</tbody>
</table>

* Please see list of acceptable technical elective courses in the course listings section

Total: 36
Post-baccalaureate Certificate Programs

Application Requirements and Process

All applicants must meet the following criteria:

- Have at least 12 months of professional work experience in information technology, security or audit.
- Be employed or have current access to an organizational environment that allows you to apply the concepts and hands-on technical skills learned in your program of study.

Applicants should follow the admissions process outlined below.

Admissions Application Form and Application Fee


A nonrefundable application fee of $100.00 must be submitted with your application. The Application Fee must be paid via credit card, U.S. currency or check, international money order, or an international check in U.S. funds drawn on a bank in the United States.

Send checks to:

SANS Technology Institute
8120 Woodmont Ave., Suite 310
Bethesda, MD 20814

Or call 301-654-7267 with your credit card information, and explain that you are making payment for the admission fee of $100.

Applications will not be considered without payment of the application fee.

Official Transcript(s)

Please have your college/university submit official transcripts directly to:

SANS Technology Institute
Attn: Master's Program - Applications
PO Box 130957
Dallas, TX 75313

For prospective students applying from outside of the United States:

Although based in Maryland, the SANS Technology Institute's programs serves students in all states and many countries around the world. When presenting a non-US transcript for admissions, candidates must first have their transcripts evaluated by World Education Services http://www.wes.org/students/index.asp before completing their submission to STI.

Résumé

Please send a current résumé that highlights your related work experience in information technology, security, or audit.

Outcome Essay

If you seek enroll in the Cybersecurity Engineering Core graduate certificate program, write a single-page, single-spaced, typed "Outcomes Statement" Essay describing how the certificate program will fit within your career development. We will evaluate your "Outcomes Statement" primarily to evaluate the quality of your writing, relative to the requirements in the Cybersecurity Engineering Core program for two 15-20 page research project/papers.

If English is not Applicant’s Native Language:

- The Test of English as a Foreign Language (TOEFL) is required for Applicants whose native language is not English. We require a minimum score requirement of 100 (Internet-based test) over-all with each of the sub-categories (Reading, Listening, Speaking, Writing) preferred to be at a minimum of 25 each. The test scores must be sent to us directly by the testing agency. The TOEFL Bulletin of Information and registration form can be obtained at American embassies and consulates, offices of the United States Information Service (USIS) and U.S. education commissions.

Applicants who cannot obtain a TOEFL Bulletin and registration form locally, may request them from:

TOEFL/TSE Services
P.O. Box 6151
Princeton, NJ 08541-6151 USA
1-609-771-7100 or 1-877-3546 or 1-609-771-7714

TOEFL Web Site  http://www.toefl.com/
• IELTS can be used as a substitute for TOEFL. We require a minimum score requirement of 7.5 over-all with each of the sub-categories in IELTS preferred to be at a minimum of 7.5 each. IELTS scores must be sent to us directly by the testing agency.
• If you are a resident alien, please enclose a copy of your appropriate documentation with your application.

Application Submission

The completed Application for Admission and supporting credentials should be emailed to admissions@sans.edu, or if necessary, may be mailed to:

The SANS Technology Institute
Attn: Graduate Program Admissions
PO Box 130957
Dallas, TX 75313

We will notify you within five business days of receiving your complete application package.

• Application Packages will be reviewed by SANS Technology Institute’s Admissions Committee.
• All information and materials furnished may be verified to preserve the integrity of the Institute, and each Applicant may be scheduled for a prequalification telephone/online (or in-person if convenient) interview.

Invitation to Matriculate

Once the Admissions Committee reviews and approves your application for admission, the Enrollment Management office will send you an "Offer of Admission," requiring your signature and return. This "Offer of Admission" letter will be contingent on two additional elements:

• First, working in concert with the Provost or another student advisor, you must complete a Program of Study plan, noting in detail where and when you intend to take courses during the first twelve months of your program participation, and generally how you will complete the program in the subsequent years.
• Second, this planning conversation must also address the student’s ability to fund his or her anticipated program of studies. The purpose of this conversation is to ensure the student recognizes the investment - both time and resources - required to complete the program. Once the applicant and Provost agree and sign off on an acceptable Program of Study plan, the applicant will return this signed Program of Study plan along with his or her counter-signed offer of admission, and will be formally matriculated.

Course Requirement Waivers (Optional)
If you have passed a GIAC certification in the last three years, you will qualify for a waiver of both that exam and the associated SANS class in any given graduate certificate program. For example, if you have passed the GIAC GCIH exam in the past three years and you enroll in the Penetration Testing & Ethical Hacking certificate program, you would qualify for a waiver from having to re-take both SANS SEC 504 and the GCIH exam as part of ISE 5200, but would need to complete the NetWars Continuous requirement. Thereafter, you could earn the certificate by taking the three additional graduate courses.

Because students must earn no less than 25% of the credits associated with a graduate certificate program directly from the SANS Technology Institute, the SANS Technology Institute can offer matriculated students a waiver for no more than one certification exam. Unfortunately, even if a student had previously taken the incorporated SANS classes and GIAC certifications in the past, we cannot grant you the graduate certificate from the SANS Technology Institute, and graduate certificates cannot be award retroactively.

Cybersecurity Engineering Core

The Cybersecurity Engineering Core certificate program spans from an introductory survey of fundamental information security tools and techniques to a more advanced study of the inter-relationships between offensive (attack/penetration testing) and defensive (intrusion detection and incident response) information security best practices. Courses in the program familiarize the student with essential tools and techniques used in cybersecurity engineering, teach the student various cyber attack techniques which may be employed in penetration testing and incident response, and reinforce a practitioner’s ability to detect attacks through packet analysis and intrusion detection. Student capabilities are reinforced through multiple hands-on labs and network simulations.

Program Learning Outcomes

The Program Learning Outcomes of the Cybersecurity Engineering Core certificate program are:

- Students will be able to utilize a broad range of current tools and technologies in the design and implementation of security solutions deployed across organizations.
- Students will be able to analyze network traffic to extract the observable characteristics of networks and network devices, thus providing a basis for defensive strategies.
- Students will be able to assemble tools and configure systems and networks to permit systems to foster resiliency and continuity of operations through attacks.
- Students will be able to understand important attacker techniques, engage in penetration testing within their organization, and respond to incidents associated with these activities within their organization.

Cybersecurity Engineering Core Graduation Requirements
The Cybersecurity Engineering Core post-baccalaureate certificate program targets completion of 12 credit hours with a 3.0 G.P.A, within 18-24 months. Students must complete the following requirements:

<table>
<thead>
<tr>
<th>Required Courses</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISE 5100 Enterprise Information Security</td>
<td>4</td>
</tr>
<tr>
<td>ISE 5200 Hacking Techniques &amp; Incident Response</td>
<td>4</td>
</tr>
<tr>
<td>ISE 5400 Advanced Network Intrusion Detection &amp; Analysis</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>12</strong></td>
</tr>
</tbody>
</table>

**Penetration Testing & Ethical Hacking**

The Penetration Testing & Ethical Hacking graduate certificate curriculum advances the student’s knowledge of the strategies and techniques utilized by hackers to gain access to networks and systems, and builds on this base to allow students to further specialize their knowledge within different types of vulnerable networks and systems. Students must take a core penetration testing and incident handling course, two additional courses focused on penetration testing of networks and web applications, and then students may choose a further specialization from courses focused on mobile, wireless, or advance network penetration testing and incident handling. Students will demonstrate deep technical knowledge in identifying and analyzing risks while providing solutions to minimize the risk.

**Program Learning Outcomes**

The program learning outcomes of the Penetration Testing & Ethical Hacking graduate certificate are designed to ensure that students are able to:

- Conduct vulnerability scanning and exploitation of various systems and applications using a careful, documented methodology to provide explicit proof of the extent and nature of IT infrastructure risks, conducting these activities according to well-defined rules of engagement and a clear scope.
- Provide documentation of activities performed during testing, including all exploited vulnerabilities and how those vulnerabilities were combined into attacks to demonstrate business or institutional risk.
- Produce an estimated risk level for a given discovered flaw by using the amount of effort the team needed to expend in penetrating the information system as an indicator of the penetration resistance of the system.
- Provide actionable results with information about possible remediation measures for the successful attacks performed.
Penetration Testing & Ethical Hacking Graduation Requirements

The Penetration Testing & Ethical Hacking post-baccalaureate certificate program targets completion of 13 credit hours with a 3.0 G.P.A, within 18-24 months. Students must complete the following requirements:

<table>
<thead>
<tr>
<th>Required Courses</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISE 5200 Hacking Techniques &amp; Incident Response</td>
<td>4</td>
</tr>
<tr>
<td>ISE 6315 Web Application Penetration Testing and Ethical Hacking</td>
<td>3</td>
</tr>
<tr>
<td>ISE 6320 Network Penetration Testing and Ethical Hacking</td>
<td>3</td>
</tr>
<tr>
<td>Penetration Testing elective (1 course)</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>13</td>
</tr>
</tbody>
</table>

Penetration Testing Elective Course Options

Students in the Penetration Testing & Ethical Hacking program must choose one course from the following list:

ISE 6325 Mobile Device Security and Ethical Hacking – 3 Credits
ISE 6330 Wireless Ethical Hacking, Penetration Testing, and Defenses – 3 Credits
ISE 6360 Advanced Penetration Testing, Exploits, and Ethical Hacking – 3 Credits

Incident Response

The graduate certificate program in Incident Response is designed to provide students with knowledge of attack vectors and techniques, the capabilities to seek out, identify and counter these attacks at both the host and network levels, and the ability in particular to examine and reverse engineer malicious code often supporting these attacks. The program introduces students to forensic analysis policy and procedures, forensic analysis tools, data recovery, and investigation techniques.

Program Learning Outcomes

The program learning outcomes of the Incident Response graduate certificate program are:

- The student will be able to explain the role of digital forensics and incident response in the field of information security, and recognize the benefits of applying these practices to both hosts and networks when investigating a cyber incident.
- The student will be able to analyze the structure of common attack techniques in order to evaluate an attacker’s footprint, target the ensuing investigation and incident response, and anticipate and mitigate future activity.
• The student will be able to evaluate the effectiveness of available digital forensic tools and use them in a way that optimizes the efficiency and quality of digital forensic investigations.
• The student will be able to utilize multiple malware analysis approaches and tools to understand how malware programs interact with digital environments and how they were coded, in order to reverse the effects of the program on networks and systems.

Incident Response Graduation Requirements

The Incident Response post-baccalaureate certificate program targets completion of 13 credit hours with a 3.0 G.P.A, within 18-24 months. Students must complete the following requirements:

<table>
<thead>
<tr>
<th>Required Courses</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISE 5200 Hacking Techniques &amp; Incident Response</td>
<td>4</td>
</tr>
<tr>
<td>ISE 6425 Advanced Computer Forensic Analysis and Incident Response</td>
<td>3</td>
</tr>
<tr>
<td>ISE 6440 Advanced Network Forensics and Analysis</td>
<td>3</td>
</tr>
<tr>
<td>ISE 6460 Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>13</strong></td>
</tr>
</tbody>
</table>
Course Listings and Descriptions

Information Security Engineering

**ISE 5000 Research & Communications Methods**  
SANS class: MGT 305 Research & Communications Methods  
0.5 Credit Hours

ISE 5000 covers strategies for conducting research and the oral and written communication that follows. The class allows the student to refine their ability to research and write professional quality reports, and to create and deliver oral presentations. Topics such as developing a convincing argument, synthesizing research and writing technical reports for non-technical audiences, and managing the communication environment are covered. Students participate in an editing exercise as well as a hands-on report writing and presentation development workshop, with a required oral presentation assessment.

**ISE 5100 Enterprise Information Security**  
SANS class: SEC 401 Security Essentials Boot-camp Style  
4 Credit Hours

ISE 5100 is the introductory, technically-oriented survey course in the information security engineering master’s program. It establishes the foundations for designing, building, maintaining and assessing security functions at the end-user, network and enterprise levels of an organization. The faculty instruction, readings, lab exercises, exam, and required student paper are coordinated to introduce and develop the core technical, management, and enterprise-level capabilities that will be developed throughout the information security engineering master’s program.

**ISE 5200 Hacking Techniques & Incident Response**  
SANS class: SEC504 Hacker Techniques, Exploits & Incident Handling  
4 Credit Hours

By adopting the viewpoint of a hacker, ISE 5200 provides an in-depth focus into the critical activity of incident handling. Students are taught how to manage intrusions by first looking at the techniques used by attackers to exploit a system. Students learn responses to those techniques, which can be adopted within the framework of the incident handling process to handle attacks in an organized way. The faculty instruction, lab exercises, exam, and NetWars simulation are coordinated to develop and test a student’s ability to utilize the core capabilities required for incident handling.

**ISE 5300 Building Security Awareness**  
SANS class: MGT 433 Securing the Human: Building and Deploying an Effective Security Awareness Program  
1 Credit Hour
One of the most effective ways to secure the human factor in an enterprise is an active awareness and education program that goes beyond compliance and leads to actual changes in behaviors. In ISE 5300, students learn the key concepts and skills to plan, implement, and maintain an effective security awareness programs that make organizations both more secure and compliant. In addition, metrics are introduced to measure the impact of the program and demonstrate value. Finally, through a series of labs and exercises, students develop their own project and execution plan, so they can immediately implement a customized awareness program for their organization.

**ISE 5400 Advanced Network Intrusion Detection & Analysis**
SANS class: SEC 503 Intrusion Detection In-Depth
4 Credit Hours

ISE 5400 arms you with the core knowledge, tools, and techniques to prepare you to defend your networks. Hands-on exercises supplement the course book material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All exercises have two different approaches. A basic one that assists you by giving hints for answering the questions. The second approach provides no hints, permitting you to have a more challenging experience.

**ISE 5500 Research Presentation 1**
1 Credit Hour

ISE 5500 gives students the ability to convert written material to a persuasive oral presentation such as might be appropriate in an enterprise environment. Students use research material written in a previous course in the curriculum to build and deliver a 30-minute presentation, typically given at a SANS training conference.

**ISE 5600 IT Security Leadership Competencies**
SANS class: MGT 514.5 IT Security Strategic Planning, Policy, and Leadership
1 Credit Hour

ISE 5600 covers the critical processes to be employed by technical leaders to develop the skills and techniques to select, train, equip, and develop a team into a single cohesive unit with defined roles that operate together in harmony toward team-objective accomplishment. Topics covered include: leadership development, coaching and training, employee involvement, conflict resolution, change management, vision development, motivation, communication skills, self-direction, brainstorming techniques, and the ten core leadership competencies.

**ISE 5700 Situational Response Practicum**
1 Credit Hour

In ISE 5700, a small group of students is given an information security scenario that is partly based on current events, and requires a broad knowledge of information security concepts. Their task is to evaluate the scenario
and to recommend a course of action. This experience is a timed 24-hour event and culminates in a group written report and presentation at the end of the 24-hour preparation time.

**ISE 5800 IT Security Project Management**  
SANS class: MGT 525 IT Project Management, Effective Communication, and PMP® Exam Prep  
3 Credit Hours

In ISE 5800 you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. The course utilizes project case studies that highlight information technology services as deliverables. ISE 5800 follows the basic project management structure from the PMBOK® Guide 5th edition and also provides specific techniques for success with information assurance initiatives. All aspects of IT project management are covered - from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes.

**ISE 5900 Research Presentation 2**  
1 Credit Hour

ISE 5900 gives a chance to further develop their skills at converting written material into a persuasive oral presentation such as might be appropriate in an enterprise environment. Students use research material written from previous courses in the curriculum to build and deliver a 30-minute presentation, either at a SANS training conference, or in an online environment.

**ISE 6000 Standards Based Implementation of Security**  
SANS class: SEC 566 Implementing and Auditing the Twenty Critical Security Controls  
4 Credit Hours

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. ISE 6000 will help you to ensure that your organization has an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches. As threats evolve, an organization’s security should too. Standards based implementation takes a prioritized, risk-based approach to security and shows you how standardized controls are the best way to block known attacks and mitigate damage from successful attacks.

**ISE 6100 Security Project Practicum**  
2 Credit Hours

In ISE 6100, a small group of students is given an information security project that requires a broad knowledge of information security concepts. Their task is to evaluate the project assignment and to recommend a course of action. This experience is a timed 30-day event. Students receive the project assignment from faculty, and must respond with a project plan to address the assignment within 5 days. The group then uses their plan to address the assignment, and deliver a written report at the end of the 30-day period.
Electives:

**ISE 6215 Advanced Security Essentials**  
SANS class: SEC 501 Advanced Security Essentials - Enterprise Defender  
3 Credit Hours

ISE 6215 reinforces the theme that prevention is ideal, but detection is a must. Students will learn how to ensure that their organizations constantly improve their security posture to prevent as many attacks as possible. A key focus is on data protection, securing critical information no matter whether it resides on a server, in robust network architectures, or on a portable device.

Despite an organization's best effort at preventing attacks and protecting its critical data, some attacks will still be successful. Therefore students will also learn how to detect attacks in a timely fashion through an in-depth understanding the traffic that flows on networks, scanning for indications of an attack. The course also includes instruction on performing penetration testing, vulnerability analysis, and forensics.

**ISE 6220 Network Perimeter Protection**  
SANS class: SEC 502 Perimeter Protection In-Depth  
3 Credit Hours

ISE 6220 provides a comprehensive analysis of a wide breadth of technologies. In fact, this is probably the most diverse course in the STI catalog, as mastery of multiple security techniques is required to defend networks from remote attacks. The course moves beyond a focus on single operating systems or security appliances. The course teaches that a strong security posture must be comprised of multiple layers. The course was developed to give students the knowledge and tools necessary at every layer to ensure their network is secure.

**ISE 6230: Securing Windows and Resisting Malware**  
SANS class: SEC 505 Securing Windows and Resisting Malware  
3 Credit Hours

ISE 6230 shows students how to secure Windows and how to minimize the impact of these changes on users of these changes. Through live demonstrations of the important steps, students follow along on their laptops. Where other courses focus on detection or remediation after the fact, the goal of this course is to prevent the infection in the first place. Students learn to write PowerShell scripts, but don't need any prior scripting experience.

**ISE 6235: Securing Linux/Unix**  
SANS class: SEC 506 Securing Linux/Unix  
3 Credit Hours
ISE 6235 provides students with experience in in-depth coverage of Linux and Unix security issues, examining how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix. This course provides specific configuration guidance and practical, real-world examples, tips, and tricks.

**ISE 6315: Web App Penetration Testing and Ethical Hacking**  
SANS class: SEC 542 Web App Penetration Testing and Ethical Hacking  
3 Credit Hours

ISE 6315 is a highly technical information security course in offensive strategies where students learn the art of exploiting Web applications so they can find flaws in enterprise Web apps before they are otherwise discovered and exploited. Through detailed, hands-on exercises students learn the four-step process for Web application penetration testing. Students will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. They then utilize cross-site scripting attacks to dominate a target infrastructure in a unique hands-on laboratory environment. Finally students explore various other Web app vulnerabilities in-depth with tried-and-true techniques for finding them using a structured testing regimen.

**ISE 6320: Network Penetration Testing and Ethical Hacking**  
SANS class: SEC 560 Network Penetration Testing and Ethical Hacking  
3 Credit Hours

ISE 6320 prepares students to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively. Students will participate in an intensive, hands-on Capture the Flag exercise, conducting a penetration test against a sample target organization.

**ISE 6325: Mobile Device Security**  
SANS class: SEC 575 Mobile Device Security and Ethical Hacking  
3 Credit Hours

ISE 6325 helps students resolve their organization’s struggles with mobile device security by equipping them with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course teaches students to build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in their organization.

**ISE 6330: Wireless Penetration Testing**  
SANS class: SEC 617 Wireless Ethical Hacking, Penetration Testing, and Defenses  
3 Credit Hours
ISE 6330 takes an in-depth look at the security challenges of many different wireless technologies, exposing students to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, students will navigate through the techniques attackers use to exploit WiFi networks, Bluetooth devices, and a variety of other wireless technologies. Using assessment and analysis techniques, this course will show students how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

ISE 6360: Advanced Network Penetration Testing
SANS class: SEC 660 Advanced Penetration Testing, Exploits, and Ethical Hacking
3 Credit Hours

ISE 6360 builds upon ISE 6320 – Network Penetration Testing and Ethical Hacking. This advanced course introduces students to the most prominent and powerful attack vectors, allowing students to perform these attacks in a variety of hands-on scenarios. This course is an elective course in the Penetration Testing & Ethical Hacking certificate program, and an elective choice for the master’s program in Information Security Engineering.

ISE 6420: Computer Forensic Investigations - Windows
SANS class: FOR 408 Computer Forensic Investigations - Windows In-Depth
3 Credit Hours

ISE 6105 Computer Forensic Investigations – Windows focuses on the critical knowledge of the Windows Operating System that every digital forensic analyst needs to investigate computer incidents successfully. Students learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations or civil/criminal litigation. The course covers the methodology of in-depth computer forensic examinations, digital investigative analysis, and media exploitation so each student will have complete qualifications to work as a computer forensic investigator helping to solve and fight crime.

ISE 6425: Advanced Computer Forensic Analysis and Incident Response
SANS class: FOR 508 Advanced Computer Forensic Analysis and Incident Response
3 Credit Hours

ISE 6420 teaches the necessary capabilities for forensic analysts and incident responders to identify and counter a wide range of threats within enterprise networks, including economic espionage, hacktivism, and financial crime syndicates. The course shows students how to work as digital forensic analysts and incident response team members to identify, contain, and remediate sophisticated threats-including nation-state sponsored Advanced Persistent Threats and financial crime syndicates. Students work in a hands-on lab developed from a real-world targeted attack on an enterprise network in order to learn how to identify what data might be stolen and by whom, how to contain a threat, and how to manage and counter an attack.

ISE 6440: Advanced Network Forensic Analysis
SANS class: FOR 572 Advanced Network Forensics and Analysis
3 Credit Hours

ISE 6440 focuses on the most critical skills needed to mount efficient and effective post-incident response investigations. Moving beyond the host-focused experiences in ISE 6420 and ISE 6425, ISE 6440 covers the tools, technology, and processes required to integrate network evidence sources into investigations, covering high-level NetFlow analysis, low-level pcap exploration, and ancillary network log examination. Students will employ a wide range of open source and commercial tools, exploring real-world scenarios to help the student learn the underlying techniques and practices to best evaluate the most common types of network-based attacks.

**ISE 6460: Malware Analysis and Reverse Engineering**
SANS class: FOR 610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
3 Credit Hours

ISE 6425 teaches students how to examine and reverse engineer malicious programs – spyware, bots, Trojans, etc. – that target or run on Microsoft Windows, within browser environments such as JavaScript or Flash files, or within malicious document files (including Word and PDF). The course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools. The malware analysis process taught in this class helps students understand how incident responders assess the severity and repercussions of a situation that involves malicious software and plan recovery steps. Students also experience how forensics investigators learn to understand key characteristics of malware discovered during the examination, including how to establish indicators of compromise (IOCs) for scoping and containing the incident.

**ISE 6615: Defending Web Applications Security Essentials**
SANS class: DEV 522 Defending Web Applications Security Essentials
3 Credit Hours

ISE 6615 covers the OWASP Top 10 and provides students with a better understanding of web application vulnerabilities, enabling them to properly defend organizational web assets. Mitigation strategies from an infrastructure, architecture, and coding perspective are discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities is also covered so students can ensure their application is tested for the vulnerabilities discussed in class.

**ISE 6715 Auditing Networks, Perimeters and Systems**
SANS class: AUD 507 Auditing Networks, Perimeters, and Systems
3 Credit Hours

ISE 6715 is organized specifically to provide a risk driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high level audit issues and general audit best practice, students have the opportunity to dive deep into the technical how to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatably verify
these controls and techniques for continuous monitoring and automatic compliance validation are given from real world examples.

**ISE 6720 Legal Issues in Data Security and Investigations**  
SANS class: LEG 523 Legal Issues in Information Technology and Security  
3 Credit Hours

ISE 6720 introduces students to the new laws on privacy, e-discovery, and data security so students can bridge the gap between the legal department and the IT department. It also provides students with skills in the analysis and use of contracts, policies, and records management procedures.

**ISE 6900 Information Security Fieldwork**  
0.5 Credit Hours

In ISE 6900, students move into the field to prepare and present on a project that will help increase computer security awareness. Students devise their own project content, based upon a defined need. Students are also responsible for inviting an audience to review the results of their project work. It is expected that at least one representative from the student's own organization (place of employment) will be present to provide evidence of the presentation.

**MSISE Capstone**  
0 Credit Hours

The GSE exam Capstone experience has two parts. The first is a multiple choice exam which may be taken at a proctored location just like any other GIAC exam. Passing this exam qualifies students to sit for the GSE hands-on lab. The first day of the two day GSE lab consists of an incident response scenario that requires the candidate to analyze data and report their results in a written report. The second consists of a rigorous battery of hands-on exercises drawn from a variety of information security domains listed.

**Information Security Management**

**ISM 5000 Research & Communications Methods**  
SANS class: MGT 305 Research & Communications Methods  
0.5 Credit Hours

ISM 5000 covers strategies for conducting research and the oral and written communication that follows. The class allows the student to refine their ability to research and write professional quality reports, and to create and deliver oral presentations. Topics such as developing a convincing argument, synthesizing research and writing technical reports for non-technical audiences, and managing the communication environment are covered. Students participate in an editing exercise as well as a hands-on report writing and presentation development workshop, with a required oral presentation assessment.
ISM 5100 Enterprise Information Security  
SANS class: MGT 512 Security Leadership Essentials  
4 Credit Hours

ISM 5100 is the introductory, survey course in the information security management master’s program. It establishes the foundations for developing, assessing and managing security functions at the end-user, network and enterprise levels of an organization. The faculty instruction, readings, exam, and required student paper are coordinated to introduce and develop the core technical, management, and enterprise-level capabilities that will be developed throughout the master’s program.

ISM 5200 Hacking Techniques & Incident Response  
SANS class: SEC504 Hacker Techniques, Exploits & Incident Handling  
4 Credit Hours

By adopting the viewpoint of a hacker, ISM 5200 provides an in-depth focus into the critical activity of incident handling. Students are taught how to manage intrusions by first looking at the techniques used by attackers to exploit a system. Students learn responses to those techniques, which can be adopted within the framework of the incident handling process to handle attacks in an organized way. The faculty instruction, lab exercises, exam, and NetWars simulation are coordinated to develop and test a student’s ability to utilize the core capabilities required for incident handling.

ISM 5300 Building Security Awareness  
SANS class: MGT 433 Securing the Human: Building and Deploying an Effective Security Awareness Program  
1 Credit Hour

One of the most effective ways to secure the human factor in an enterprise is an active awareness and education program that goes beyond compliance and leads to actual changes in behaviors. In ISM 5300, students learn the key concepts and skills to plan, implement, and maintain an effective security awareness programs that make organizations both more secure and compliant. In addition, metrics are introduced to measure the impact of the program and demonstrate value. Finally, through a series of labs and exercises, students develop their own project and execution plan, so they can immediately implement a customized awareness program for their organization.

ISM 5400 IT Security Planning, Policy & Leadership  
SANS class: MGT 514 IT Security Strategic Planning, Policy, and Leadership  
4 Credit Hours

ISM 5400 covers the entire strategic planning process: how to plan the plan, horizon analysis, visioning, environmental scans (SWOT, PEST, Porter's etc.), historical analysis, mission, vision, and value statements. The course also reviews the planning process core, candidate initiatives, the prioritization process, resource and IT change management in planning, how to build a roadmap, setting up assessments, and revising the plan.
ISM 5500 Research Presentation 1
1 Credit Hour

ISE 5500 gives students the ability to convert written material to a persuasive oral presentation such as might be appropriate in an enterprise environment. Students use research material written in a previous course in the curriculum to build and deliver a 30-minute presentation, typically given at a SANS training conference.

ISM 5600 Legal Issues in Data Security and Investigations
SANS class: LEG 523 Legal Issues in Information Technology and Security
4 Credit Hours

ISM 5600 introduces students to the new laws on privacy, e-discovery, and data security so students can bridge the gap between the legal department and the IT department. It also provides students with skills in the analysis and use of contracts, policies, and records management procedures.

ISM 5700 Situational Response Practicum
1 Credit Hour

In ISE 5700, a small group of students is given an information security scenario that is partly based on current events, and requires a broad knowledge of information security concepts. Their task is to evaluate the scenario and to recommend a course of action. This experience is a timed 24-hour event and culminates in a group written report and presentation at the end of the 24-hour preparation time.

ISM 5800 IT Security Project Management
SANS class: MGT 525 IT Project Management, Effective Communication, and PMP® Exam Prep
3 Credit Hours

In ISM 5800 you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. The course utilizes project case studies that highlight information technology services as deliverables. ISM 5800 follows the basic project management structure from the PMBOK® Guide 5th edition and also provides specific techniques for success with information assurance initiatives. All aspects of IT project management are covered - from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes.

ISM 5900 Research Presentation 2
1 Credit Hour

ISE 5900 gives a chance to further develop their skills at converting written material into a persuasive oral presentation such as might be appropriate in an enterprise environment. Students use research material written from previous courses in the curriculum to build and deliver a 30-minute presentation, either at a SANS training conference, or in an online environment.
**ISM 6000 Standards Based Implementation of Security**  
SANS class: SEC 566 Implementing and Auditing the Twenty Critical Security Controls  
4 Credit Hours

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. ISM 6000 will help you to ensure that your organization has an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches. As threats evolve, an organization’s security should too. Standards based implementation takes a prioritized, risk-based approach to security and shows you how standardized controls are the best way to block known attacks and mitigate damage from successful attacks.

**ISM 6100 Security Project Practicum**  
2 Credit Hours

In ISM 6100, a small group of students is given an information security project that requires a broad knowledge of information security concepts. Their task is to evaluate the project assignment and to recommend a course of action. This experience is a timed 30-day event. Students receive the project assignment from faculty, and must respond with a project plan to address the assignment within 5 days. The group then uses their plan to address the assignment, and deliver a written report at the end of the 30-day period.

**ISM 6200 Auditing Networks, Perimeters and Systems**  
SANS class: AUD 507 Auditing Networks, Perimeters, and Systems  
4 Credit Hours

ISM 6200 is organized specifically to provide a risk driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high level audit issues and general audit best practice, students have the opportunity to dive deep into the technical how to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatably verify these controls and techniques for continuous monitoring and automatic compliance validation are given from real world examples.

**ISM 6900 Information Security Fieldwork**  
0.5 Credit Hours

In ISM 6900, students move into the field to prepare and present on a project that will help increase computer security awareness. Students devise their own project content, based upon a defined need. Students are also responsible for inviting an audience to review the results of their project work. It is expected that at least one representative from the student's own organization (place of employment) will be present to provide evidence of the presentation.

**MSISM Capstone**  
Assessment: GSM  
0 Credit Hours
The GSM exam Capstone experience is a two day hands-on lab exercise where students demonstrate their ability to formulate and implement policies and solutions that demonstrate a thorough understanding of security foundations and practical applications of information technology. Students work through scenarios which require them to: construct information security approaches that balance organizational needs, apply standards-based approaches to information security risk management, and devise incident response strategies.

**Technical Elective Course Options**
(Masters candidates only)

The following is a list of acceptable technical elective courses. Students in the MSISE program must choose 3 courses from this list. Students in the MSISM program must choose 1 course from this list.

- ISE 6215: Advanced Security Essentials
- ISE 6220 Network Perimeter Protection
- ISE 6230: Securing Windows and Resisting Malware
- ISE 6235: Securing Linux/Unix
- ISE 6315: Web App Penetration Testing and Ethical Hacking
- ISE 6320: Network Penetration Testing and Ethical Hacking
- ISE 6325: Mobile Device Security
- ISE 6330: Wireless Penetration Testing
- ISE 6360: Advanced Penetration Testing
- ISE 6420: Computer Forensic Investigations - Windows
- ISE 6425: Advanced Computer Forensic Analysis and Incident Response
- ISE 6440: Advanced Network Forensics and Analysis
- ISE 6460: Malware Analysis and Reverse Engineering
- ISE 6615: Defending Web Applications Security Essentials
- ISE 6715 Auditing Networks, Perimeters and Systems
- ISE 6720 Legal Issues in Data Security and Investigations (MSISE students only)

**Technology and Software Requirements**

In order to fulfill the requirements of the STI course curriculum, you are expected to have, or have access to:

- A personal computer capable of connecting to the internet
- An email account
- A word-processor software program such as *Microsoft Word*, *iWork Pages*, or *Open Office Writer*
- A web-browser (Internet Explorer, Firefox, Chrome, etc.)

In addition, most of your classes will require special software to be loaded on your computer. Approximately a week before class, you will receive notice of that class’ software requirements. This will tell you where to get any software needed for the class and labs, as well as any configuration settings that need to be applied.