SANS Technology Institute

2021 Graduate Course Catalog

SANS Technology Institute
11200 Rockville Pike, Suite 200
North Bethesda, MD 20852

WWW.SANS.EDU | INFO@SANS.EDU

TABLE OF CONTENTS

Academic Calendar

SANS Technology Institute students choose from a variety of online and live course delivery options. Students begin their distance courses on the 1st and 15th of each month or live courses on various dates offered throughout the year. While the dates of terms are individualized for each student, the length of each term is standardized and varies only based on the specific courses students are enrolled in. Though students enjoy this flexible enrollment model, student progress and enrollment reporting is based on a semi-annual semester cycle,1/1 - 6/30, and 7/1 - 12/31.

Course lengths are detailed below in the Course Listings and Descriptions section, and full-time requirements are listed in the Student Handbook.

Our offices are closed on: New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving and the Friday after Thanksgiving, and Christmas Eve and Day.

2021 Select Live Learning Event Schedule

*Due to the COVID-19 pandemic, live events that are currently scheduled for 2021 may be offered virtually.

Event	Start Date
Spring Semester Cycle	
SANS Security East	January, 2021
Cyber Threat Intelligence Summit	January, 2021
SANS Cyber Security West	February, 2021
Pen Test & Offensive	February, 2021
SANS	March, 2021
Leadership & Cloud	March, 2021
SANS Baltimore Spring	April, 2021
SANSFIRE	June, 2021
Fall Semester Cycle	
SANS Columbia	July, 2021
SANS Baltimore Fall	September, 2021
SANS Network Security	September, 2021
Pen Test HackFest Summit	November, 2021
SANS Cyber Defense Initiative	December, 2021

The full schedule of upcoming events is available online at: https://www.sans.org/security-training/by-location/north-america.

Tuition and Fees

Students pay tuition on a per course basis and are required to pay tuition at the time of registration for each course. In the master's degree program, the cost of tuition is based off a per credit hour rate while in the graduate certificate programs, tuition is a flat rate per course.

All course materials are included in the cost of tuition and are provided to the student directly. Students taking courses using one of the distance modalities (OnDemand, Live Online) will have course materials shipped to the address on file in their SANS account. Students attending live events will pick up their course materials during conference check-in.

Discounts or promotions offered by SANS Institute, including the SANS Work Study Program, do not apply to graduate course tuition.

The following tables reflect the tuition rates by program, dependent upon when a student was admitted to the program.

Master's Degree

Program	Cost per Credit	Capstone Fee*	Total Credits	Total Cost
M.S. in Information Security Engineering	$1,375	$1,375	36	$49,500
(admitted ***between*** 3/1/2019-8/31/2020)	$1,375	$3,000	36	$51,125
(admitted ***prior to*** 3/1/2019)	$1,250	$3,000	36	$46,750
M.S. in Information Security Management	$1,250	$2,100	35	$47,100

Post-Baccalaureate Certificate Programs

Program	Cost per Course	Cost of Practicum	Total Credits	Total Cost
Cybersecurity Engineering (Core)	$5,500	$1,375	13	$23,375
*(admitted **between** 3/1/2019-6/30/2020)*	$5,500	$4,125	12	$20,625
*(admitted **prior** to 3/1/2019)*	$5,000	*Included*	12	$15,000
Penetration Testing & Ethical Hacking	$5,500	$1,375	13	$23,375
*(admitted **prior** to 3/1/2019)*	$5,000	*Included*	13	$20,000
Incident Response	$5,500	$1,375	13	$23,375
*(admitted **prior** to 3/1/2019)*	$5,000	*Included*	13	$20,000
Cyber Defense Operations	$5,500	n/a	12	$22,000
*(admitted **prior** to 3/1/2019)*	$5,000	n/a	12	$20,000
Industrial Control Systems Security	$5,500	n/a	12	$22,000
*(admitted **prior** to 3/1/2019)*	$5,000	n/a	12	$20,000
Purple Team Operations	$5,500	$5,500	15	$27,500
Cybersecurity Management	$5,500	n/a	15	$27,500

Single Courses, Non-degree Seeking Students

Students enrolled in a single course as a non-degree seeking student pay a flat tuition rate per course of $6,000. For any student, there is a lifetime cap of two courses as a non-degree seeking student.

Fees

The following fees may apply:

Application Fee*	$35 (Graduate Certificate) $100 (Master's)
GIAC Exam Retake Fee	$799

* Paid during the application process

Cancellation and Change Fees

SANS.edu students who wish to cancel and receive a refund for a particular graduate course must submit a request by email to their student advisor. Requests must be received 45 days before the start of the course. Payments will be refunded by the method that they were submitted and a processing fee of $300 will be deducted. Requests received within 45 days of the start of the course may not receive a refund, but credit towards enrollment in a future course.

Students who seek to change the venue, timing, or modality for a course should submit a change request by email to their student advisor. Requests must be received 45 days before the start of the course. Processing fees may apply.

No cancellations or changes will be made once:

- Online course materials have been accessed
- Print course materials have been mailed to the student
- The student has arrived at a live event

Cancellation Fee	$300 processing fee
Course Change Fee	$150 processing fee

Students using VA Education Benefits may cancel a course up to 7 days prior to the start of a course without incurring any cancellation or change fees. For cancellations within 7 days of a course starting, students will be responsible for paying cancellation or change fees. Refunds of military education benefits will be resolved via the VA's Debt Management Center. As part of any such refund, any overpayment received by the student (e.g., Chapter 30 tuition payments or Chapter 33 book or housing stipend) will be the responsibility of the affected student.

Capstone Cancellation

Cancellation of any approved registration for the GSE in-person lab within 45 days prior to the start of the lab will be subject to forfeiture of the full lab fee.

Cost of Live Learning Events

Travel and Lodging

Students are responsible for the costs of hotel, food, and travel should they attend a live SANS event as part of their coursework. The average hotel and food cost, if the hotel rooms are not shared, is $1,800 per event ($200 per night for accommodations and $100 per day for food), though significant savings are available through room sharing. These amounts are to be paid directly to the hotel at which the learning event is being conducted.

Live Class Add-ons

Students attending live SANS events have the option to add supplemental items, such as an OnDemand bundle or a 2-day summit pass, to their registration. As these items are not program requirements, they are not included in graduate course tuition and will incur an additional cost to the student. If interested, students should ask their advisor how to add these items to their registration.

Student Veterans will find that these add-ons are not covered by VA Education Benefits.

Financial Aid/Title IV Eligibility

The SANS Technology Institute is approved by the US Department of Education as an eligible Title IV institution. While we do not participate in Title IV funded student loan programs, eligibility status permits us to, from the date of eligibility forward, offer the following opportunities to our students:

- Provide a 1098-T to students who are funding part of their program cost in order for them to file for possible tax credit.
- Students may be eligible to utilize 529 educational funds where there is a state requirement for Title IV eligibility.
- Students may be eligible to utilize corporate or employer tuition reimbursement programs where Title IV eligibility is required.

Veterans Benefits

The SANS Technology Institute is authorized by the Department of Veterans Affairs to accept VA Education Benefits. Students using VA Education Benefits are responsible for any tuition not paid to SANS.edu directly by the VA by the end of their course term. Please refer to the Veterans Benefits section towards the end of this catalog for more detailed information.

Programs of Study

The SANS Technology Institute offers the following programs of study, at the graduate level:

- Master of Science in Information Security Engineering
- Master of Science in Information Security Management
- Post-baccalaureate certificate: Cybersecurity Engineering (Core)
- Post-baccalaureate certificate: Penetration Testing & Ethical Hacking
- Post-baccalaureate certificate: Incident Response
- Post-baccalaureate certificate: Cyber Defense Operations
- Post-baccalaureate certificate: Industrial Control Systems Security
- Post-baccalaureate certificate: Purple Team Operations
- Post-baccalaureate certificate: Cybersecurity Management

Master's Degree Programs

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.

Program Learning Outcomes

The program learning outcomes of the MSISE program are designed to ensure that students are 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.

Curriculum

The M.S. in Information Security Engineering is a 36-credit hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 5101	Security Essentials	3
ISE 5201	Hacking Techniques & Incident Response	3
ISE 5601	IT Security Leadership Competencies	3
ISE 6255	Defensible Security Architecture & Engineering	3
ISE 5300	Managing Human Risk	1
ISE 5401	Advanced Network Intrusion Detection & Analysis	3
ISE 5701	Situational Response Practicum	1
ISE 6200	Core Comprehensive Exam	1
ISE 5800	IT Security Project Management	3
ISE 6999	Elective Courses *Students choose three electives from an approved list of courses.*	9
ISE 6300	NetWars Continuous Practicum	1
ISE 5901	Advanced Technical Research & Communication Practicum	3
ISE 6101	Security Project Practicum	1
ISE 6901	MSISE Capstone	1

Focus Areas

Master's candidates may elect to focus their elective courses in a particular area. If choosing a focus area, the student must select the following elective courses:

Focus Area	Available Elective Courses
Cyber Defense Operations	*Choose 3 from:* ISE 6215, ISE 6230, ISE 6240, ISE 6250, ISE 6255
Penetration Testing	*Choose 3 from:* ISE 6315, ISE 6320, ISE 6325, ISE 6330, ISE 6350, ISE 6360
Incident Response	*Choose 3 from:* ISE 6420, ISE 6425, ISE 6440, ISE 6445, ISE 6450, ISE 6460
Security Management	ISE 6720, ISE 6715, and any other elective from the approved catalog
Industrial Control Systems	ISE 6515, ISE 6525, ISE 6520

Full course descriptions can be found later in this catalog.

Master of Science in Information Security Management

The Master of Science in Information Security Management (MSISM) Program is designed to accelerate the development of information security managers by providing practical experience that can be applied immediately on the job. Students learn from the industry experts how to see the world from an attacker's view, audit information systems, assess legal implications of an incident, and develop risk-based secure enterprise-level solutions that enable an organization's business processes to function in spite of the increasing threat presence. In addition to developing hands-on technical skills, the program emphasizes the development of communication and leadership skills that will improve the student's ability to implement information security solutions within their organization.

Program Learning Outcomes

The program learning outcomes of the MSISM program are designed to ensure that students are 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.

- Assess and balance the relationship and inter-responsibilities between all three communities of interest in Information Security: General Business, Information Technology, and Information Security.
- 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.

Curriculum

The M.S. in Information Security Management is a 35-credit hour program, comprised of the following courses:

Required Courses		**Credits**
ISM 5101	Security Essentials	3
ISM 5201	Hacking Techniques & Incident Response	3
ISM 5300	Manging Human Risk	1
ISM 5400	IT Security Strategic Planning, Policy, and Leadership	3
ISM 5501*	Technical Research & Communication Practicum	3
ISM 5601	Law of Data Security and Investigations	3
ISM 5700	Situational Response Practicum	1
ISM 5800	IT Security Project Management	3
ISM 6001	Standards-based Implementation of Security	3
ISM 5901*	Advanced Technical Research & Communication Practicum	3
ISM 6100	Security Project Practicum	1
ISM 6201	Auditing Networks, Perimeters and Systems	3
ISM 6300	Core NetWars Continuous Practicum	1
ISE 6999	Elective Course**	3
N/A	MSISM Capstone	1

*ISM 5501 & ISM 5901 replaces previous RES 5500/ISM 5550 & RES 5900/ISM 5900 practicums
**Please see list of acceptable technical elective courses in the course listings section

Full course descriptions can be found later in this catalog.

Post-baccalaureate Certificate Programs

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) graduate certificate are designed to ensure that students are able to:

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

Curriculum

The post-baccalaureate certificate program in Cybersecurity Engineering Core is a 12-credit hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 5101 **ISE 6215**	Security Essentials Advanced Security Essentials *Students select one of these survey courses*	3
ISE 5201	Hacking Techniques and Incident Response	3
ISE 5401	Advanced Network Intrusion Detection and Analysis	3
ISE 6999	Elective Course *Students choose an elective from an approved list of courses.*	3
ISE 6200	Capstone: Core Comprehensive Exam	1

Full course descriptions can be found later in this catalog.

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.

Curriculum

The post-baccalaureate certificate program in Penetration Testing & Ethical Hacking is a 13-credit hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 5201	Hacking Techniques & Incident Response	3
ISE 6315	Web Application Penetrating Testing & Ethical Hacking	3
ISE 6320	Network Penetration Testing & Ethical Hacking	3
ISE 6999	Elective Course	3
ISE 6300	Core NetWars Continuous Capstone	1

Elective Course Options

Students will choose one of the following courses as their elective:
ISE 6325, ISE 6330, ISE 6350, ISE 6360

Full course descriptions can be found later in this catalog.

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 are designed to ensure that students are able to:

- 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.

Curriculum

The post-baccalaureate certificate program in Incident Response is a 13-credit hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 6420	Computer Forensic Investigations - Windows	3
ISE 6425	Advanced Computer Forensic Analysis & Incident Response	3
ISE 6440	Advanced Network Forensics & Analysis	3
ISE 6999	Elective Courses *Students choose an elective from an approved list of courses.*	3
ISE 6400	DFIR NetWars Continuous Capstone	1

Full course descriptions can be found later in this catalog.

Elective Course Options

Students will choose one of the following courses as their electives:
ISE 5201, ISE 6445, ISE 6450, ISE 6460

Cyber Defense Operations

The graduate certificate in Cyber Defense Operations provides a path for professionals to specialize in a sub-area of the information security field, and this progression of courses in defensive techniques is made available just as they would be to a candidate for the master's degree in Information Security Engineering. Armed with a deep understanding of layered defense-in-depth techniques used by government and private sector organizations to protect their critical assets, the professional who earns the Cyber Defense Operations post-baccalaureate certificate will be empowered to identify and help remediate their organization's vulnerabilities.

Program Learning Outcomes

The program learning outcomes of the Cyber Defense Operations graduate certificate are designed to ensure that students are able to:

- Utilize a broad range of current tools and technologies in the design and implementation of security solutions deployed across organizations.
- Identify the information assets of an enterprise, classify them by value, and determine what management and technical controls can be used to monitor and audit them effectively.
- Develop a program for analyzing the risk to the information assets in an enterprise and determining which technical and management controls can mitigate, remove, or transfer that risk.
- Articulate important attacker techniques, analyze the traffic that flows on networks, and identify indications of an attack, engage in penetration testing within their organization, and respond to incidents associated with these activities within their organization.

Curriculum

The post-baccalaureate certificate program in Cyber Defense Operations is a 12-credit hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 6240	Continuous Monitoring and Security Operations	3
ISE 5401	Advanced Network Intrusion Detection and Analysis	3
ISE 6999	Elective Course I	3
ISE 6999	Elective Course II	3

Elective Course Options

Students will choose two of the following courses as their electives:
ISE 6001, ISE 6215, ISE 6230, ISE 6250 ISE 6255

Full course descriptions can be found later in this catalog.

Industrial Control Systems Security

The Industrials Control Systems Security graduate certificate program provides a broad and integrated mechanism for students to learn the essential security awareness, work-specific knowledge, and hands-on technical skills needed to secure automation and control system technology.
These systems often form the backbone of infrastructures identified as critical to national security, economic security, public health, or safety. Traditional defenses found in business or corporate IT environments are not always effective when applied to the industrial or operation technology space. Legacy equipment, proprietary hardware and software, non-traditional protocols, and consideration for the health and safety of equipment, personnel, and communities all add to the challenges of securing these environments.

Program Learning Outcomes

The program learning outcomes of the Industrial Control Systems Security graduate certificate are designed to ensure that students are able to:

- Learn, integrate, practice, and demonstrate mastery of the essential knowledge, technical skills, and leadership abilities relevant to securing automation and control system technology.
- Utilize a broad range of current tools and technologies in the design and implementation of security solutions deployed across critical infrastructure organizations.
- Identify the information assets within an automation or control systems environment, classify them by value, and determine what management and technical controls can be used to monitor and audit them effectively and securely.
- Develop a program for analyzing the risk to the information assets in an automation or control systems environment and determine which technical and management controls can mitigate, remove, or transfer that risk.
- Articulate important attacker techniques, analyze the traffic that flows on automation or control system networks, and identify indications of an attack, engage in testing and audit within their organization, and respond to incidents associated with these activities within their organization.

Curriculum

The post-baccalaureate certificate program in Industrial Control Systems Security is a 12-credit hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 6515	ICS/SCADA Security Essentials	3
ISE 6520	ICS Active Defense and Incident Response	3
ISE 6525	Essentials for NERC Critical Infrastructure Protection	3
ISE 6999	Elective Course *Students choose an elective from an approved list of courses.*	3

Full course descriptions can be found later in this catalog.

Purple Team Operations

The Post-Baccalaureate Certificate in Purple Team Operations is a 15-credit hour program with a cohesive set of learning outcomes focused on teaching blue and red applied concepts, skills, and technologies used in a merged fashion in the current best practice known as purple operations, or purple teams. This program is intended for experienced information security practitioners who are interested in rounding out their blue and red skills so as to be able to effectively operate and lead at the intersection of those domains.

Program Learning Outcomes

The primary educational objectives of the program are to:

- Practice and demonstrate mastery of fundamental network security knowledge and skills.
- Understand, practice, and demonstrate mastery of important defensive techniques and identify indications of an attack in order to detect / respond to/ mitigate incidents on enterprise networks.
- Understand, practice, and demonstrate mastery of important attacker techniques and be able to utilize the full range of penetration techniques in order to breach a network, pivot within it, and disrupt, exploit, or exfiltrate data from it.
- Utilize a broad range of both blue team and red team tools, technologies, and mindsets in the integrated design and implementation of purple security activities and exercises in order to maximize the synergy of full spectrum security operations.

Curriculum

The post-baccalaureate certificate program in Purple Team Operations is a 15-credit hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 6310	Enterprise Threat and Vulnerability Assessment	3
ISE 6215	Advanced Security Essentials	3
ISE 6999	Students will select one Blue Team Elective	3
ISE 6999	Students will select one Red Team Elective	3
ISE 6250	Capstone: Purple Team Tactics & Kill Chain Defenses	3

Elective Course Options

Students will choose one of the following courses as their Blue Team Elective:
ISE 5401, ISE 6240

Students will choose one of the following courses as their Red Team Elective:
ISE 6320, ISE 6360

Full course descriptions can be found later in this catalog.

Cybersecurity Management

The Post-baccalaureate Certificate in Security Management is a 15-credit hour program with a cohesive set of learning outcomes focused on preparing experienced information security practitioners to become effective managers and leaders. Security Management certificate students will complete three required core courses and two elective courses, earning five industry-recognized GIAC certifications.

Program Learning Outcomes

The program learning outcomes of the Cybersecurity Management graduate certificate are designed to ensure that students are able to:

- Manage the information security function in an enterprise in a way that takes into account the relationship between and responsibilities shared by the communities of interest in an enterprise. These include the general business, information technology, and information security.
- 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, implementation programs, and personnel-into an operation that can effectively manage the security needs of an enterprise.
- Articulate positions on the legal issues associated with the protection of information and privacy that meet generally accepted ethical standards and the security and business needs of the enterprise.
- Devise strategies and programs for incident detection and response, including business continuity planning and disaster recovery planning (BCP/DRP), that are cost effective and meet the business needs of the enterprise.

Curriculum

The post-baccalaureate certificate program in Cybersecurity Management is a 15-credit hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 5001	Security Leadership Essentials for Managers	3
ISE 6255	Defensible Security Architecture and Engineering	3
ISE 5650	Security Strategic Planning, Policy, Business Fundamentals, and Leadership	3
ISE 6999	Elective Course	3
ISE 6999	Elective Course	3

Elective Course Options

Students will choose one of the following courses as their elective:
ISE 6001, ISE 5800, ISE 6715, ISE 6720

Full course descriptions can be found later in this catalog.

Course Listings and Descriptions

Information Security Engineering

ISE 5001: Security Leadership Essentials for Managers
SANS MGT 512 | GIAC GSLC | 3 Credit Hours | 90 Days

Restrictions | *This course is only available in the Cybersecurity Management Program.*

ISE 5001 is the introductory, survey course in the cybersecurity management certificate program. MGT512 covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls are covered in conjunction with key management topics that address the overall security lifecycle, including governance and technical controls focused on protecting, detecting, and responding to security issues.

ISE 5101: Security Essentials
SANS SEC 401 | GIAC GSEC | 3 Credit Hours | 90 Days

ISE 5101 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, and exam are coordinated to introduce and develop the core technical, management, and enterprise-level capabilities that will be developed throughout the rest of the certificate program.

ISE 5201: Hacker Tools, Techniques, Exploits, & Incident Handling
SANS SEC 504 | GIAC GCIH | 3 Credit Hours | 90 Days

By adopting the viewpoint of a hacker, ISE 5201 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 and exam are coordinated to develop and test a student's ability to utilize the core capabilities required for incident handling.

ISE 5600: IT Security Planning, Policy, & Leadership
SANS MGT 514 (Sections 3 – 5) | 1 Credit Hour | 45 Days

Restrictions | *This course is only available OnDemand, and part of MSISE Curriculum 3.4 and below.*

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, strategic planning and policy development, and the ten core leadership competencies.

ISE 5601: IT Security Planning, Policy, & Leadership
SANS MGT 514 **|** GIAC GSTRT | 3 Credit Hours | 90 Days

ISE 5601 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, strategic planning and policy development, and the ten core leadership competencies.

ISE 5650: IT Security Planning, Policy, & Leadership
SANS MGT 514, SEC 405 **|** GIAC GSTRT | 3 Credit Hours | 90 Days

Restrictions | *This course is only available in the Cybersecurity Management Program.*

ISE 5650 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, strategic planning and policy development, and the ten core leadership competencies. This course additionally includes the content from SEC 405, Business Finance Essentials.

ISE 6255: Defensible Security Architecture and Engineering
SANS SEC 530 **|** GIAC GDSA **|** 3 Credit Hours | 90 Days

Effective security requires a balance between detection, prevention, and response capabilities. Defensible Security Architecture and Engineering is designed to help students establish and maintain a holistic and layered approach to security. Students will learn the fundamentals of up-to-date defensible security architecture and how to engineer it, with a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to significantly improve their organization's prevention capabilities in the face of today's dynamic threat landscape. The course will also delve into the latest technologies and their capabilities, strengths, and weaknesses. Multiple hands-on labs conducted daily will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

ISE 5300: Managing Human Risk
SANS MGT 433 | SANS SSAP Exam | 1 Credit Hour | 45 Days

Restrictions | *This course is only available through SANS OnDemand.*

From phishing attacks and credential stuffing to lost devices or auto-complete in email, human risk has become the primary risk for most organizations. One of the most effective ways for an organization to manage its human risk is to build on their existing technical controls with a mature security awareness program. The program must go beyond just compliance and change organizational behaviors and ultimately, culture. In ISE/ISM 5300, you will learn the key concepts and skills to plan, maintain, and measure an effective security awareness program that makes an

organization both more secure and compliant. Through a series of labs and exercises, you will develop your security awareness plan and also complete the SSAP exam.

ISE 5401: Intrusion Detection In-Depth
SANS SEC 503 | GIAC GCIA | 3 Credit Hours | 90 Days

ISE 5401 arms students with the core knowledge, tools, and techniques to detect and analyze network intrusions, building in breadth and depth for advanced packet and traffic analysis. Hands-on exercises supplement the course book material, allowing students to transfer the knowledge in their heads to their keyboards 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.

ISE 5501: Technical Research & Communication Practicum
3 Credit Hours | 120 Days* *Following approval of the student's initial proposal

Restrictions | *This course is part of MSISE Curriculum 3.4 and below.*

ISE 5501 is a graduate-level research and presentation course in which students will identify, investigate and analyze a problem. Students will write a whitepaper interpreting the data collected and making recommendations for action. The whitepaper will reflect original work towards a new practice, solution, tool, policy, or paradigm offering the potential for real impact in the field of information security.

Students will then convert written material to an oral presentation in order to inform a technical audience about the topic. Delivered via a webinar, students use material from their paper to build and deliver a 30-minute presentation and to then field questions. Students demonstrate a variety of presentation skills. Exemplary presentations may be selected to present at a live SANS event for further professional development.

ISE 5700 Situational Response Practicum
1 Credit Hour | 30 Days

Restrictions | *This course is part of MSISE Curriculum 3.4 and below.*

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 course begins with a timed 24-hour event which culminates in a group written report and presentation. Students have 30 days following the practicum to submit an additional written assignment.

ISE 5701 Situational Response Practicum
SANS SEC 402, SEC 405 | 1 Credit Hour | 45 Days

Restrictions | *SEC 402 and SEC 405 must be taken through SANS OnDemand.*

The purpose of this course is for students to learn and be assessed on their ability to come together as a team, assess a situation, develop a response and prepare recommendations for decision to a C-Level audience within forty-five (45) days. You are put into a small group with other students and

presented with an information security topic prompt. Your group then prepares a plan for researching and reporting on the assignment. Once the plan is prepared, the group executes the plan, adjusting as necessary, to develop a report of the research completed recommended actions.

ISE 6200: MSISE Program Midterm
Core Comprehensive Exam | 1 Credit Hour | 30 Days

The Core Comprehensive Exam determines if candidates have mastered the core technical skills required by top security consultants and individual practitioners. Through a series of exercises, students demonstrate their ability to integrate the knowledge, skills and techniques acquired in ISE 5101, ISE 5201, and ISE 5401 to address common challenges faced by technical leaders in the cybersecurity field.

ISE 5800: IT Security Project Management
SANS MGT 525 | GIAC GCPM | 3 Credit Hours | 90 Days

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 6300 NetWars Continuous Practicum
1 Credit Hour | 60 Days

NetWars Continuous is an online training program that guides students through hands-on lessons to locate vulnerabilities, exploit diverse machines, and analyze systems. NetWars provides a forum to test and perfect cyber security skills in a manner that is legal and ethical. Students will face challenges derived from real-world environments and actual attacks that businesses, governments, and military organizations must deal with every day.

ISE 6100 Security Project Practicum
1 Credit Hour | 30 Days

Restrictions | *This course is part of MSISE Curriculum 3.4 and below.*

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.

ISE 6101 Security Project Practicum
SANS SEC 403 | 1 Credit Hour | 30 Days

The purpose of this course is for students to learn and be assessed on their ability to come together as a team, assess a situation, demonstrate leadership, develop a response and prepare and present recommendations for a decision to a C-Level audience within 24-hours. This course builds on what you have learned in other courses and allows you to apply that knowledge. You are put into a small group with other students and presented with an information security topic prompt. Working as a group, you will analyze the situation, develop a technical response, and develop recommendations for an organizational response to the situation presented. Upon development of your recommended response, the group provides written and oral reports of recommendations for action to a mixed technical/non-technical audience of executives for decision.

ISE 5901 Advanced Technical Research & Communication Practicum
3 Credit Hours | 120 Days* *Following approval of the student's initial proposal

ISE 5901 is an advanced graduate-level research and presentation course in which students will identify, investigate and analyze a problem. Students will write a whitepaper interpreting the data collected and making recommendations for action. The whitepaper will reflect original work towards a new practice, solution, tool, policy, or paradigm offering the potential for real impact in the field of information security.

Students will then convert written material to an oral presentation in order to inform a technical audience about the topic. Delivered via a webinar, students use material from their paper to build and deliver a 30-minute presentation and to then field questions. Students demonstrate a variety of presentation skills. Exemplary presentations may be selected to present at a live SANS event for further professional development.

ISE 6901: MSISE Capstone
GIAC GSE Entrance Exam **|** 1 Credit Hour **|** 90 Days

The MSISE capstone is comprised of the GSE entrance exam, which may be taken at a proctored location just like any other GIAC. Passing this exam qualifies students to sit for the GSE hands-on lab, though the lab is not required in the MSISE program.

ISE 6400 DFIR NetWars Continuous Practicum
1 Credit Hour | 60 Days

Restrictions | *This course is only available for students pursuing a graduate certificate in Incident Response.*

DFIR NetWars Continuous is an incident simulator packed with a vast amount of forensic, malware analysis, threat hunting, and incident response challenges designed to help you gain proficiency without the risk associated when working real-life incidents.

ISE 7000: MSISE Capstone
GIAC GSE Entrance Exam and Lab **|** 1 Credit Hour **|** 180 Days

Restrictions | *This course is part of MSISE Curriculum 3.3 and below.*

The MSISE capstone is comprised of the GSE entrance exam, which may be taken at a proctored location just like any other GIAC, and a hands-on lab, which is completed in person.

Technical Elective Course Options

The following are 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 6001: Implementing & Auditing the Critical Security Controls
SANS SEC 566 | GIAC GCCC | 3 Credit Hours | 90 Days

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. ISE 6001 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 6215: Advanced Security Essentials
SANS SEC 501 | GIAC GCED | 3 Credit Hours | 90 Days

Students will learn how to design and build a secure network that can both prevent attacks and recover after a compromise. They will also learn how to retrofit an existing network to achieve the level of protection that is required. While prevention is important to learn, students will also learn how to detect the indications that the attack is in progress and stop it before significant harm is caused. Packet analysis and intrusion detection are at the core of this study. In the third module, students will learn about the variety of tests that can be run against an organization and how to perform effective penetration testing. To round out the defensive posture, students will learn the practice of identifying, analyzing, and responding effectively to attacks, including the identification of malware and steps that can be taken to prevent data loss.

ISE 6230: Securing Windows & PowerShell Automation
SANS SEC 505 | GIAC GCWN | 3 Credit Hours | 90 Days

ISE 6230 shows students how to secure servers, workstations and portable devices running Microsoft Windows. Windows is the most frequent target of hackers and advanced malware. While other courses focus on detection or remediation of a compromise after the fact, the aim of this course is to substantially reduce these compromises in the first place. For scalability and automation, this course includes many hands-on labs with Group Policy and PowerShell scripting. No prior scripting experience is required. Learning at least the basics of PowerShell is an essential skill for anyone who manages Windows servers or clients in an enterprise.

ISE 6240: Continuous Monitoring & Security Operations
SANS SEC 511 | GIAC GMON | 3 Credit Hours | 90 Days

A new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses. ISE 6240 teaches this new proactive approach and strengthens student's skills to undertake that proactive approach. The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation

(CDM)/Continuous Security Monitoring (CSM) taught in this course will help students best position their organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior.

ISE 6245: SIEM with Tactical Analytics
SANS SEC 555 **|** GIAC GCDA **|** 3 Credit Hours | 90 Days

This course is designed to demystify the Security Information and Event Management (SIEM) architecture and process, by navigating the student through the steps of tailoring and deploying a SIEM to full Security Operations Center (SOC) integration.

ISE 6250: Purple Team Tactics & Kill Chain Defenses
SANS SEC 599 | GIAC GDAT | 3 Credit Hours | 90 Days

ISE 6250 leverages the purple team concept by bringing together red and blue teams for maximum effect. Recognizing that a prevent-only strategy is not sufficient, the course focuses on current attack strategies and how they can be effectively mitigated and detected using a Kill Chain structure. Throughout the course, the purple team principle will be maintained, where attack techniques are first explained in-depth, after which effective security controls are introduced and implemented.

ISE 6310: Enterprise and Cloud | Threat Vulnerability
SANS SEC 460 | GIAC GEVA | 3 Credit Hours | 90 Days

Restrictions | *This course is only available in the Purple Team Operations Certificate.*

ISE 6310 covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy. ISE 6310 teaches the use of industry standard security tools for vulnerability assessment, management, and mitigation. The student will learn on a full scale enterprise cyber range of target machines representative of an enterprise environment, leveraging production ready tools and a proven testing methodology. This course also emphasizes a personnel centric approach to security by examining the shortfalls of many vulnerability assessment programs in order to provide the student with the tactics and techniques required to secure networks against even the most advanced intrusions. The course concludes with a discussion of triage, remediation, and reporting before putting the student's skills to the test on the final day against an enterprise grade cyber range with numerous target systems to analyze and explore. The cyber range is a large environment of servers, end-users, and networking gear that represents many of the systems and topologies used by enterprises.

ISE 6315: Web App Penetration Testing and Ethical Hacking
SANS SEC 542 | GIAC GWAPT | 3 Credit Hours | 90 Days

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 SEC 560 | GIAC GPEN | 3 Credit Hours | 90 Days

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 & Ethical Hacking
SANS SEC 575 | GIAC GMOB | 3 Credit Hours | 90 Days

ISE 6325 helps students resolve their organization's struggles with mobile device security by equipping then 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 & Ethical Hacking
SANS SEC 617 | GIAC GAWN | 3 Credit Hours | 90 Days

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 6350: Python for Penetration Testers
SANS SEC 573 | GIAC GPYC | 3 Credit Hours | 90 Days

The ISE 6350 course teaches student in the pen testing specialization, and other students who want to use the Python programming language, how to enhance their overall effectiveness during information security engagements. Students will learn how to apply core programming concepts and techniques learned in other courses through the Python programming language. The course teaches skills and techniques that can enhance an information security professional in penetration tests, security operations, and special projects. Students will create simple Python-based tools to interact with network traffic, create custom executables, test and interact with databases and websites, and parse logs or sets of data.

ISE 6360: Advanced Penetration Testing, Exploit Writing, & Ethical Hacking
SANS SEC 660 | GIAC GXPN | 3 Credit Hours | 90 Days

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 FOR 500 | GIAC GCFE | 3 Credit Hours | 90 Days

ISE 6420 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 Digital Forensics, Incident Response, & Threat Hunting
SANS FOR 508 | GIAC GCFA | 3 Credit Hours | 90 Days

ISE 6425 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 FOR 572 | GIAC GNFA | 3 Credit Hours | 90 Days

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 6445: Cyber Threat Intelligence
SANS FOR 578 | GIAC GCTI | 3 Credit Hours | 90 Days

ISE 6445 will equip you, your security team, and your organization in the tactical, operational, and strategic level cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and to accurately and effectively counter those threats. This course focuses on structured analysis in order to establish a solid foundation for any security skillset and to amplify existing skills.

ISE 6450: Advanced Smartphone Forensics
SANS FOR 585 | GIAC GASF | 3 Credit Hours | 90 Days

The focus of ISE 6450 is on teaching students how to perform forensic examinations on devices such as mobile phones and tablets. Students will add to their forensics skills with this course's focus on the advanced skills of mobile forensics, device file system analysis, mobile application behavior, event artifact analysis and the identification and analysis of mobile device malware. Students will learn how to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features a number of hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools.

ISE 6460: Reverse-Engineering Malware
SANS FOR 610 | GIAC GREM | 3 Credit Hours | 90 Days

ISE 6460 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 6515: ICS/SCADA Security Essentials
SANS ICS 410 | GIAC GICSP | 3 Credit Hours | 90 Days

ISE 6515 ICS/SCADA Security Essentials is an introductory study of the information technology and operational technology roles that have converged in today's industrial control system environments. This convergence has led to a greater need for a common understanding between the various groups who support or rely on these systems. Students in ISE 6515 will learn the language, the underlying theory, and the basic tools for industrial control system security in settings across a wide range of industry sectors and applications.

ISE 6520: ICS Active Defense and Incident Response
SANS ICS 515 | GIAC GRID | 3 Credit Hours | 90 Days

ISE 6520 will empower students to understand their networked industrial control system environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations.

ISE 6525: Essentials for NERC Critical Infrastructure Protection

SANS ICS 456 | GIAC GCIP | 3 Credit Hours | 90 Days

ISE 6525 empowers students with knowledge of the "what" and the "how" of the version 5/6 standards. The course addresses the role of FERC, NERC and the Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

ISE 6615: Defending Web Applications Security Essentials
SANS SEC 522 | GIAC GWEB | 3 Credit Hours | 90 Days

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 6650: Cloud Security and DevOps Automation
SANS SEC 540 | GIAC GCSA | 3 Credit Hours | 90 Days

Restrictions | *This course is only available as an elective within the MSISE or MSISM program.*

ISE 6650 provides development, operations, and security professionals with a methodology to build and deliver secure infrastructure and software using DevOps and cloud services. Students will explore how the principles, practices, and tools of DevOps can improve the reliability, integrity, and security of on-premise and cloud-hosted applications. Starting with on-premise deployments, the first two days of the course examine the Secure DevOps methodology and its implementation using lessons from successful DevOps security programs. Students will gain hands-on experience using popular open-source tools to automate Configuration Management ("infrastructure as Code"), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance ("Compliance as Code"), and Continuous Monitoring. After laying the DevSecOps foundation, the final three days move DevOps workloads to the cloud, build secure cloud infrastructure, and deliver secure software.

ISE 6715: Auditing & Monitoring Networks, Perimeters, & Systems
SANS AUD 507 | GIAC GSNA | 3 Credit Hours | 90 Days

Restrictions | *This course is only available as an elective within the MSISE program or Cybersecurity Management Certificate.*

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 LEG 523 | GIAC GLEG | 3 Credit Hours | 90 Days

Restrictions | *This course is only available as an elective within the MSISE program or Cybersecurity Management Certificate.*

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.

Information Security Management

ISM 5101: Security Essentials
SANS MGT 512 | GIAC GSLC | 3 Credit Hours | 90 Days

ISM 5101 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 writing assignment are coordinated to introduce and develop the core technical, management, and enterprise-level capabilities that will be developed throughout the master's program.

ISM 5201: Hacking Techniques & Incident Response
SANS SEC 504 | GIAC GCIH | 3 Credit Hours | 90 Days

By adopting the viewpoint of a hacker, ISM 5201 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, and exam are coordinated to develop and test a student's ability to utilize the core capabilities required for incident handling.

ISM 5300: Managing Human Risk
SANS MGT 433 | SANS SSAP Exam | 1 Credit Hour | 45 Days

Restrictions | *This course is only available through SANS OnDemand.*

From phishing attacks and credential stuffing to lost devices or auto-complete in email, human risk has become the primary risk for most organizations. One of the most effective ways for an organization to manage its human risk is to build on their existing technical controls with a mature security awareness program. The program must go beyond just compliance and change organizational behaviors and ultimately, culture. In ISE/ISM 5300, you will learn the key concepts and skills to plan, maintain, and measure an effective security awareness program that makes an organization both more secure and compliant. Through a series of labs and exercises, you will develop your security awareness plan and also complete the SSAP exam.

ISM 5400: IT Security Planning, Policy & Leadership
SANS MGT 514 | 3 Credit Hours | 90 Days

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 5501: Technical Research & Communication Practicum
3 Credit Hours | 120 Days* *Following approval of the student's initial proposal

ISE 5501 is a graduate-level research and presentation course in which students will identify, investigate and analyze a problem. Students will write a whitepaper interpreting the data collected and making recommendations for action. The whitepaper will reflect original work towards a new practice, solution, tool, policy, or paradigm offering the potential for real impact in the field of information security.

Students will then convert written material to an oral presentation in order to inform a technical audience about the topic. Delivered via a webinar, students use material from their paper to build and deliver a 30-minute presentation and to then field questions. Students demonstrate a variety of presentation skills. Exemplary presentations may be selected to present at a live SANS event for further professional development.

ISM 5601: Legal Issues in Data Security and Investigations
SANS LEG 523 | GIAC GLEG | 3 Credit Hours | 90 Days

ISM 5601 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 | 30 Days

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 course begins with a timed 24-hour event which culminates in a group written report and presentation. Students have 30 days following the practicum to submit an additional written assignment.

ISM 5800: IT Security Project Management
SANS MGT 525 | GIAC GCPM | 3 Credit Hours | 90 Days

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 5901: Advanced Technical Research & Communication Practicum
3 Credit Hours | 120 Days* *Following approval of the student's initial proposal

ISE 5901 is an advanced graduate-level research and presentation course in which students will identify, investigate and analyze a problem. Students will write a whitepaper interpreting the data collected and making recommendations for action. The whitepaper will reflect original work towards a new practice, solution, tool, policy, or paradigm offering the potential for real impact in the field of information security.

Students will then convert written material to an oral presentation in order to inform a technical audience about the topic. Delivered via a webinar, students use material from their paper to build and deliver a 30-minute presentation and to then field questions. Students demonstrate a variety of presentation skills. Exemplary presentations may be selected to present at a live SANS event for further professional development.

ISM 6001: Standards-based Implementation of Security
SANS SEC 566 | GIAC GCCC | 3 Credit Hours | 90 Days

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. ISM 6001 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
1 Credit Hour | 30 Days

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 6201: Auditing Networks, Perimeters and Systems
SANS AUD 507 | GIAC GSNA | 3 Credit Hours | 90 Days

ISM 6201 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 repeatedly verify these controls and techniques for continuous monitoring and automatic compliance validation are given from real world examples.

ISE 6300: NetWars Continuous Practicum
1 Credit Hour | 60 Days

NetWars Continuous is an online training program that guides students through hands-on lessons to locate vulnerabilities, exploit diverse machines, and analyze systems. NetWars provides a forum to test and perfect cyber security skills in a manner that is legal and ethical. Students will face challenges derived from real-world environments and actual attacks that businesses, governments, and military organizations must deal with every day.

MSISM Capstone
GSM Exam | 1 Credit Hour

Restrictions | *The GSM lab is offered once or twice a year, dependent on need.*

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.

Admissions Requirements and Application 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 during the master's degree program.
- Have earned a baccalaureate degree from a recognized college or university, or the international equivalent, with a minimum cumulative grade point average of 2.8.

All applicants must submit the following (detailed application guidelines can be found online):

a) Application Form
b) Current Resume
c) Official Transcripts
d) Application Fee
e) Requirements for International Students
    - Transcript Evaluation through World Evaluation Services (WES)
    - Non-native English speakers must submit TOEFL Scores.

Applicants to the master's degree program must also submit:

i. Letter of Recommendation
ii. Goals and Outcomes Statement
iii. Video Presentation

Application Submission

The completed application for admission and supporting credentials should be submitted online at https://application.sans.edu/apply/.

Invitation to Matriculate

Once the Admissions Committee reviews and approves an application for admission, the Admissions Office will send an Offer of Admission. Enrollment in the SANS Technology Institute will be contingent upon successful completion of the virtual New Student Orientation within 30 days of admission.

New Student Orientation

Our New Student Orientation (NSO) ensures that all new students are provided with the information necessary to navigate their college experience successfully. It is important that students refrain from registering for their first course before completing NSO, to prevent delays and complications in registration processing. During NSO, a student will: complete an orientation module and follow-up survey, schedule an appointment with their student advisor, and finally register for their first course. Students wishing to attend an upcoming live event as part of their first course are encouraged to communicate that at the time of admission.

We recommend students set aside 30 minutes to complete the orientation module and survey and an additional 30 minutes for the academic advising appointment. For details on the start dates and preferred deadlines, please visit https://www.sans.edu/students/orientation.

Credit Transfers and Waivers

Credit Transfers

The SANS Technology Institute does not generally accept transfers of credit for coursework completed at other regionally accredited higher education institutions. Any decision to make an exception to this policy in a given individual instance would need to be approved by the faculty in conjunction with the Admissions Committee or the Executive Director.

The SANS Technology Institute may grant credit to students accepted to its master's programs who are, or had been, participants in government or military educational and training programs that are taught by SANS Technology Institute faculty and based on the same course instruction and exam requirements that are included in the master's program. In cases where this prior work represents only part of the credits and requirements of a course, the incoming student will need to complete the remaining course requirements in order to receive full credit and a course grade.

Waivers of Course Requirements

The SANS Technology Institute waives requirements for course elements or courses within its program of studies when a student has previously attained 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 and requirements as described below.

- An evaluation of waivers, indicating all course waivers, will be completed and agreed upon before matriculation.
- Waivers will not be granted when the requirements of the waiver are met *after* a student matriculates.
- 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 for the remaining components completed by the matriculated student will be used to determine the course grade.

SANS Institute Classes and GIAC Certifications

The SANS Technology Institute will grant a waiver to a student from the requirements within a graduate course to complete both a relevant SANS Institute class and GIAC exam if the student has passed the relevant GIAC exam, and the certification is current and active.

In cases where the student previously attended a SANS class but did not take/pass the associated GIAC exam, they can elect to take the GIAC exam once enrolled in the program. Students pursuing this option will register and pay tuition for the GIAC exam but will *not* receive current course materials for the associated SANS class.

GIAC Exam Challenges

Graduate students may elect to place out of a course by challenging the associated final GIAC exam without first taking the associated SANS class. In this case, the student will register and pay tuition for the exam attempt but will not receive course materials.

Master's degree students are limited to two GIAC exam challenges while graduate certificate students are limited a single GIAC exam challenge. Waivers granted for GIAC exam challenges will count against the waiver limit of one-quarter of the program's credit hours.

GIAC Gold Papers

The SANS Technology Institute will grant a waiver to a student from the requirements within a research practicum course (ISE 5501 or ISE 5901), in the event a student has successfully completed a GIAC Gold Paper within 5 years of being admitted to the program. This waiver is subject to the Gold Paper being reviewed within the Technical Research and Communication requirements.

PMP® Certification

For master's candidates 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 ISC^2 organization, a waiver will be granted within ISE/ISM 5101 for the SANS class (SEC 401 and MGT 512, respectively). Achievement of the associated GIAC certification (GSEC or GSLC) will still be required for the award of credit. Students pursuing this option will register and pay tuition for the GIAC exam but will *not* receive course materials for the SANS SEC 401 or MGT 512 class.

Technology and Software Requirements

In order to fulfill the requirements of the SANS Technology Institute 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.)
- A webcam is required to take GIAC exam remotely through ProctorU

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.

Veterans Benefits

Introduction

This section provides you with explanations for how your veterans benefits will work relative to the programs at the SANS Technology Institute (SANS.edu). In addition to the information provided here, we recommend that students review the *Student Handbook*, which contains additional academic and student conduct policies.

Background Information

Our programs are delivered in non-standard academic terms and are designed to maximize the flexibility by which a student can engage in the required coursework. Rather than taking courses on-campus during fixed semesters, our programs are delivered through a series of courses taken via a mix of modalities (primarily at a student's option), with asynchronous start dates. All students enrolled in a degree program will need to satisfy the same requirements, but the timing of individual student progression may differ according to individual schedules and the availability of courses.

PROGRAM CHARACTERISTIC	STANDARD COLLEGE	SANS TECHNOLOGY INSTITUTE
ENROLLMENT PERIOD	Typical semesters	Asynchronous start dates
STANDARD TERMS	15-19 weeks	Varying course-term lengths depending upon course
COURSE MODALITY	Either on-campus, in-person classroom instruction or 100% online	Mix of in-person and at-a-distance modalities, at the student's option

The flexible structure of our programs – course start dates, the mix of in-classroom and at-a-distance options, the varying terms for courses, their associated credit hours, and calculated pace of progress – impacts how payment benefits are calculated by the VA. As a result, there may be significant fluctuations in the payments you receive throughout the course of your program. This is not to suggest that total available benefits are enhanced or diminished, but simply that our structure may cause a variability in payments at different times as you enroll in courses, experience gaps between courses, and engage in different instructional modalities. The resulting payments will be different and less consistent than they would be if you were to attend a traditional, brick-and-mortar college with fixed semester terms and standard credit hour assignments per course.

Additionally, an individual taking a single course as a non-degree seeking student may ***not*** use their VA educational benefits to fund that course. GI Bill® benefits will only cover courses that are taken as part of a degree-granting program.

Because the rules and processes associated with VA educational benefits are complex, a full description is beyond the scope of this guide. However, we will generally distinguish between Post-9/11 GI Bill® and other sections in this guide, and will seek to point out where and how payment amounts you receive are determined by the courses you might be taking at the time.

Approved Live Learning Events for 2021*

At this time, the SANS Technology Institute is approved and eligible to receive veterans benefits only in the State of Maryland. Because of this, student veterans may apply their benefits only to courses where the instruction element is delivered live at an approved location in Maryland, or delivered at-a-distance. Resident course offerings in Maryland vary each year. Here are the approved training sites for 2021:

Baltimore:	**Columbia**:	**Bethesda**:
Hyatt Regency Baltimore	Sheraton Columbia Town Center	Hyatt Regency Bethesda
300 Light Street	10207 Wincopin Circle	One Bethesda Metro Center
Baltimore, MD 21201	Columbia, MD 21044 US	7400 Wisconsin Ave
		Bethesda, MD 20814

*Post-9/11 GI Bill® students enrolled in approved resident courses which have been converted to online learning solely due to COVID-19, will continue to receive benefits until December 21, 2021, or until the school resumes normal operations of resident training, whichever comes first.

Chapter 33 Post-9/11 GI Bill®

For Chapter 33 benefits, tuition and fees are sent directly to the school to pay for courses that have been certified. It also provides a monthly housing allowance and book stipend which are described below. Students with questions regarding specific amounts for housing allowances are encouraged to reach out to the VA directly at the GI Bill® help line (888-442-4551) or online at https://gibill.custhelp.va.gov/

Housing Allowance

The Monthly Housing Allowance (MHA) is paid directly to the student on the 1st of the month, based upon enrollment time in the previous month. MHA will be paid for periods when:

a. The student is enrolled in at least one course,
b. The student is earning credits at a 'rate of pursuit' greater than half-time, and
c. The student is not on active duty.

The calculation of MHA is impacted by the following considerations:

Course Modality

- Students who take a course in-person (in Maryland) will be paid per the calculation determined by the BAH for an "E-5 with Dependents" using the ZIP code of *the live event attended*.
- Students who take a distance education course will be paid a housing stipend at the online rate, set as roughly one-half the national average.
- More information about the MHA can be found at https://www.benefits.va.gov/GIBILL/resources/benefits_resources/rates/ch33/ch33rates080118.asp#HOUSING

'Rate of Pursuit'
As detailed earlier in the catalog, each course is itself a term, as far as enrollment is concerned. This means that when we certify terms to the VA, those terms are simply each course. Additionally, we certify terms (courses) to the VA one week before the course begins, which the deadline for any schedule changes.

- Graduate students using GI Bill® will be considered full-time in each term (course) if they pursue courses that have a 1 credit per 1 month ratio. For example, a 3-credit course taken over the 3-month period is considered full-time (3/3), while a 3-credit course taken over 4-months is less than full-time (3/4).
    - *MHA payment for courses taken at less than full-time will be determined by the VA.*
- The VA will calculate a prorated MHA amount based upon a student's benefit level, the rate of pursuit, and the number of days in a month the student was enrolled in a course.
- Students may complete coursework earlier than the targeted timeframe and we will adjust the certification to reflect the actual time taken to complete the course. These adjustments may impact MHA payments, as it relates to enrollment periods changing.

Books and Fees Stipend

The book stipend is a lump sum paid directly to the student for each enrollment certification processed, up to an annual cap. The stipend pays $41.67 per credit certified, and is prorated by your qualification percentage. The annual cap re-sets the 1st of August each year.

Vocational Rehab and Employment

Similar to the Post 9/11 GI Bill®, Vocational Rehabilitation and Employment (VR&E) benefits pay the school directly for 100% of tuition and fees. It also provides monthly housing allowance based on the students' rate of pursuit (full-time, ¾ time, etc.).

Other GI Bill® Chapters, including Chapter 30 Montgomery Bill

Other GI Bill® Chapters (30, 35, 1606) send monthly stipend payments directly to the student based on their rate of pursuit (full-time, ¾ time, etc.), who then must pay the school for tuition and fees. Eligible students who are certified for these VA benefits do not have to remit the full tuition payment at the time of registration. However, students using benefits under these chapters will be required to pay their tuition to SANS Technology Institute by the end of their course terms.

Yellow Ribbon Program

Because our typical costs do not exceed the established thresholds under the Post-9/11 GI Bill®, the SANS Technology Institute does not participate in the Yellow Ribbon Program.

Registering and Paying for Courses

Once students have completed orientation and their initial advising appointment, they are able to register for their first course and request to be certified with the VA. Here is an outline of the process:

1) After the initial advising meeting, a student advisor will email registration instructions which will prompt the students to indicate "using GI Bill" in the special comments line of the registration form. This provides SANS.edu with consent to be "certified" with the VA for the course.
2) Students should select "check" as payment method to submit registration without making a payment.
3) We will leave the invoice as "UNPAID" until payment has been received from the VA. Students may see another invoice in their SANS portal listed as "COMPED" to order the associated SANS components.
4) Students using Chapter 33 at less than 100% eligibility, or students using other Chapters, have up until the end of the course to pay tuition. Failure to have tuition paid by the end of the course term may result in academic dismissal.

Please note:

- Student Veterans do not need to use VA benefits for every course throughout the program but can instead elect to use it for only certain courses. Therefore, students need to indicate on each course registration form (as indicated in Step 1 above) if they would like to utilize their benefits.
- Many schools offer a Priority Enrollment status for students using GI Bill®. Because all students have equal registration access, SANS.edu does not have a Priority Enrollment policy in place for students using GI Bill®.

VA Requirements of GI Bill® Users

- Students who seek to use GI Bill® or VR&E must first apply for benefits online at vets.gov and submit official documentation to SANS.edu (i.e. Certificate of Eligibility or VR&E Authorization Form) at the time of admission.
- The VA will only pay for courses listed in the catalog that are required for a degree and for programs that have been approved for study by the VA.
- If students take courses in addition to those listed for their approved program, they will not be entitled to receive VA benefits for them.
- Students who do not complete a course that has been certified by the VA will owe tuition and fees back to the VA.

  Course Failures

  The VA requires schools to report whether a failing grade is the result of a student's lack of participation in the course thus, there are effectively two types of failing grades.
  - If you participate in the course (e.g. view all OnDemand material, take practice tests, comment in Canvas discussion board, submit written assignments, etc.), failing your course will not result in the VA recollecting tuition or applicable housing allowance.
  - If you did not participate in the course (e.g. stopped viewing OnDemand material, did not attempt practice tests, were not active in Canvas, etc.), then we will report your non-attendance failure to the VA, as well the last date of course activity. The VA will seek to recollect tuition and applicable housing allowance for the entire course duration.

- Students are expected to maintain satisfactory academic progress as outlined in the *Student Handbook.*

VA Requirements of SANS Technology Institute

The VA requires the SANS Technology Institute to:

Monitor Course and Program Progress
SANS.edu will monitor your course activity to ensure that you are progressing appropriately. We track course activity by checking OnDemand progress, activity in the Student Portal, practice test performance, etc. Additionally, you will be required to follow the Satisfactory Academic Progress policy as mandated by SANS.edu to remain in good standing with the institution.

Certify Enrollments (VA Form 22-1999)
We will submit VA form 22-1999 (Enrollment Certification) on the first day of class for courses taken in-classroom or via our Live Online modality, and on the 1st or 15th of the month for OnDemand courses.

Please note refunds are not given after classes begin for in-person/Live Online courses, nor after date of registration for OnDemand courses.

Report Enrollment Information
SANS.edu is required to report any changes in your enrollment status to the VA. Enrollment changes could include withdrawals, change course date, change delivery modality, etc. These changes could affect your rate of pursuit which could impact your stipend and/or benefits payments. We also report academic progress (including academic probation or dismissal), and certify graduation/program completion.

Review of School Records by VA and Maryland State Approving Agent
By law, SANS.edu is required to maintain and make available student records (such as enrollment periods, grade information, student application, etc.) to authorized representatives of the government. We will retain your records for a minimum of 3 years following the termination of your enrollment.

Students can expect the following of the VA:

Benefit Letters
The VA will mail an award (benefit) letter to you showing we certified you and indicating the amounts you will receive during the course enrollment period/term. You are advised to stay informed as to your remaining benefits, as you are responsible for any tuition the VA does not pay.

Funding Your Tuition
- For Montgomery GI Bill® (Chapter 30): The VA will deposit money directly into the bank account you have provided to them.
- For Post-9/11 GI Bill® (Chapter 33): The VA will send funds for tuition and fees directly to SANS Technology Institute and deposit funds for the book stipend and MHA to you.

VA Resources and Contact Information

While we will make every effort to help you navigate your benefits, it is ultimately your responsibility to understand your benefits. We cannot advise students on eligibility of benefits, as we do not represent the Department of Veterans Affairs. The following resources are available to help you find the information you need:

- GI Bill® Official Web Site: http://www.benefits.va.gov/gibill/
- Online benefits application portal: https://www.vets.gov/
- GI Bill® Education Forms hard copies: http://www.benefits.va.gov/gibill/handouts_forms.asp
- GI Bill® FAQ: https://gibill.custhelp.com/app/answers/list
- Payment Rates and Comparison Tool: http://www.benefits.va.gov/gibill/comparison_tool.asp
- Post-9/11 GI Bill® Summary: http://www.benefits.va.gov/gibill/post911_gibill.asp
- Harry W. Colmery Veterans Educational Assistance Act (Forever GI Bill®): https://www.benefits.va.gov/GIBILL/FGIBSummaries.asp
- Education Benefits Phone Number: 1-888-GIBILL-1 (1-888-442-4551)

GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA). More information about education benefits offered by VA is available at the official U.S. government Web site at www.benefits.va.gov/gibill.

California State Tuition Recovery Fund Disclosures

As a registered out-of-state accredited institution, and as required by California state law, the SANS Technology Institute is providing residents of California, with the following disclosures:

The State of California established the Student Tuition Recovery Fund (STRF) to relieve or mitigate economic loss suffered by a student in an educational program at a qualifying institution, who is or was a California resident while enrolled, or was enrolled in a residency program, if the student enrolled in the institution, prepaid tuition, and suffered an economic loss. Unless relieved of the obligation to do so, you must pay the state-imposed assessment for the STRF, or it must be paid on your behalf, if you are a student in an educational program, who is a California resident, or are enrolled in a residency program, and prepay all or part of your tuition.

You are not eligible for protection from the STRF and you are not required to pay the STRF assessment, if you are not a California resident, or are not enrolled in a residency program.

It is important that you keep copies of your enrollment agreement, financial aid documents, receipts, or any other information that documents the amount paid to the school. Questions regarding the STRF may be directed to the Bureau for Private Postsecondary Education, 2535 Capitol Oaks Drive, Suite 400, Sacramento, CA 95833, (916) 431-6959 or (888) 370-7589.

To be eligible for STRF, you must be a California resident or are enrolled in a residency program, prepaid tuition, paid or deemed to have paid the STRF assessment, and suffered an economic loss as a result of any of the following:

1. The institution, a location of the institution, or an educational program offered by the institution was closed or discontinued, and you did not choose to participate in a teach-out plan approved by the Bureau or did not complete a chosen teach-out plan approved by the Bureau.
2. You were enrolled at an institution or a location of the institution within the 120 day period before the closure of the institution or location of the institution, or were enrolled in an educational program within the 120 day period before the program was discontinued.
3. You were enrolled at an institution or a location of the institution more than 120 days before the closure of the institution or location of the institution, in an educational program offered by the institution as to which the Bureau determined there was a significant decline in the quality or value of the program more than 120 days before closure.
4. The institution has been ordered to pay a refund by the Bureau but has failed to do so.
5. The institution has failed to pay or reimburse loan proceeds under a federal student loan program as required by law, or has failed to pay or reimburse proceeds received by the institution in excess of tuition and other costs.
6. You have been awarded restitution, a refund, or other monetary award by an arbitrator or court, based on a violation of this chapter by an institution or representative of an institution, but have been unable to collect the award from the institution.
7. You sought legal counsel that resulted in the cancellation of one or more of your student loans and have an invoice for services rendered and evidence of the cancellation of the student loan or loans.

To qualify for STRF reimbursement, the application must be received within four (4) years from the date of the action or event that made the student eligible for recovery from STRF.

A student whose loan is revived by a loan holder or debt collector after a period of non-collection may, at any time, file a written application for recovery from STRF for the debt that would have otherwise been eligible for recovery. If it has been more than four (4) years since the action or event that made the student eligible, the student must have filed a written application for recovery within the original four (4) year period, unless the period has been extended by another act of law.

However, no claim can be paid to any student without a social security number or a taxpayer identification number."

- Collect STRF assessments (if applicable) from enrolling students
- Remit collected STRF assessments to the Bureau
- Complete and submit STRF Assessment Reporting Form to the Bureau by:

Quarter	Submission Deadline
1st	April 30th
2nd	July 31st
3rd	October 31st
4th	January 31st

Maryland Guaranty Student Tuition Fund

A student may be entitled to make a claim against the Maryland Guaranty Student Tuition Fund for For-profit Institutions of Higher Education ("Student Tuition Fund") in the case of certain events, including a school closure. The Student Tuition Fund is administered by the Maryland Higher Education Commission. Information about the Student Tuition Fund and instructions for filing a claim may found in Regulations 13B.02.06.01 through .13 of the Code of Maryland Regulations or by contacting the Maryland Higher Education Commission.