SANS Technology Institute

2021 Undergraduate 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

The SANS Technology Institute operates on a nonstandard term model. Each course enrollment is itself the course term, as students generally progress through their programs one course at a time. Though our enrollment terms are asynchronous (term starts are individualized to each student), the length of each term is still standardized and varies only based on the type of courses in which students enroll. As such, we use the calendar year as our academic year. Course lengths are detailed below in the Course Listings and Descriptions section.

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.

Class instruction may be taken in a live classroom or online, as available. The following schedule is not an exhaustive list of live classroom opportunities, but rather larger events we anticipate being most popular with students.

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	
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	
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 live events is available online at: https://www.sans.org/security-training/by-location/north-america.

Applied Cybersecurity Certificate Program

The Upper Division Undergraduate Certificate in Applied Cybersecurity (ACS) program is designed to complement and build upon the preparation students receive in community colleges, or in other undergraduate programs, and to prepare them for immediate employment.

Students in the ACS program will work towards two outcomes: (1) proficiency in the fundamental technical knowledge and skills that serve as the baseline for all professionals in cybersecurity, and (2) early specialization in advanced skills that can be applied to particular areas of information security practice.

Program Learning Outcomes

The intended learning objectives of the ACS program are to:

- Utilize a broad range of current tools and technologies in the design and implementation of defensive security solutions that may be deployed across an organization's computing and network environment.
- Assemble tools and configure systems and networks to permit systems to foster resiliency and continuity of operations through attacks.
- Understand the most prevalent methods and vectors used in cyber attacks in order to assess the vulnerabilities of an organization relative to these attack vectors, and to respond to incidents associated with these activities within their organization.
- Build upon these baseline skills and choose to begin to specialize in a particular area of information security practice associated with a more specialized and job-specific role, including advanced defensive techniques, vulnerability analysis and penetration testing, or digital forensics.

ACS Curriculum

The Upper Division Undergraduate Certificate program in Applied Cybersecurity (ACS) is a total of 12 credit hours and is made up of 3 standard courses and 1 elective course.

Required Courses		Final Exam	Credit Hours
ACS 3275	Foundations: Computers, Technology, & Security	GFACT	3
ACS 3401	Security Essentials	GSEC	3
ACS 3504	Security Incident Handling & Hacker Exploits	GCIH	3
ACS 4xxx	Elective course (choose one)	GIAC exam	3

Cyber Defense

- ACS 4450: Blue Team Fundamentals: Security Operations and Analysis (GSOC)
- ACS 4501: Advanced Security Essentials (GCED)
- ACS 4503: Intrusion Detection In-Depth (GCIA)

Penetration Testing

- ACS 4542: Web App Penetration Testing and Ethical Hacking (GWAPT)
- ACS 4560: Network Penetration Testing and Ethical Hacking (GPEN)

Digital Forensics and Incident Response

- ACS 4508: Advanced Incident Response, Threat Hunting, and Digital Forensics (GCFA)

Cloud Security

- ACS 4488: Cloud Security Essentials (GCLD)
- ACS 4510: Public Cloud Security (GPCS)

Industrial Control Systems Security

- ACS 4410: ICS/SCADA Security Essentials (GICSP)

Course Listings and Descriptions

ACS 3275: Foundations: Computers, Technology, & Security

SANS SEC 275 | *GIAC GFACT*

ACS 3275 is purpose-built to provide students with the fundamental technical knowledge and skills that serve as the baseline for all professionals in cybersecurity, reinforcing key concepts with interactive labs. You'll establish a core understanding of technology component functions and apply that knowledge to security concepts such as reconstructing a crime from digital evidence or locating exploitable flaws in software and websites. The course ensures a solid mastery of computer, hardware, network, and cybersecurity fundamentals, including the study of operating systems, Windows security tools, Linux, programming with Python and C, advanced Google searches, reconnaissance, virtualization, and encryption. You'll explore the inner workings of packets and protocols that allow the internet to function and learn the role of a computer's central processing unit (CPU), how it executes code, its relationship with memory, and the fundamentals of how attackers disrupt intended behavior.

3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)
* This course was previously numbered ACS 3201

ACS 3401: Security Essentials

SANS SEC 401 | *GIAC GSEC*

ACS 3401 is a technically-oriented survey course in which you'll learn the most effective steps to prevent cyber attacks and detect adversaries. In classes and hands-on labs, you'll learn to develop effective security metrics that provide a focused playbook that IT can implement, auditors can validate, and executives can understand. You'll explore methods to analyze and assess the risk to your environment in order to drive the creation of a security roadmap that focuses on the right areas of security. And you'll learn practical tips and tricks to focus in on high-priority security problems and on the actions required to protect and secure an organization's critical information assets and business systems.

Prerequisites: ACS 3275
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 3504: Security Incident Handling and Hacker Exploits

SANS SEC 504 | *GIAC GCIH*

ACS 3504 is 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 today.

Prerequisites: ACS 3401
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

Technical Elective Course Options

ACS 4410: Security Essentials for Industrial Control Systems
SANS ICS 410 | *GIAC GICSP*
ACS 4410 is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. Students will learn the language, the underlying theory, and the basic tools for industrial control system security in setting across a wide range of industry sectors and applications.

Prerequisites: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 4450: Blue Team Fundamentals: Security Operations and Analysis
SANS SEC 450 | *GIAC GSOC*
ACS 4450 provides students with technical knowledge and key concepts essential for security operation center (SOC) analysts and new cyber defense team members. By providing a detailed explanation of the mission and mindset of a modern cyber defense operation, this course will jumpstart and empower those on their way to becoming the next generation of blue team members.

Prerequisites: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 4488: Cloud Security Essentials
SANS SEC 488 | *GIAC GCLD*
ACS 4488 covers Amazon Web Services, Azure, Google Cloud, and other cloud service providers (CSPs). Like foreign languages, cloud environments have similarities and differences, and this course will introduce you to the language of cloud security. Upon completion of this course, you will be able to advise and speak about a wide range of cybersecurity topics and successfully navigate the challenges and opportunities presented by cloud service providers.

Prerequisites: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 4501: Advanced Enterprise Defender
SANS SEC 501 | *GIAC GCED*
ACS 4501 brings together all the elements of a modern cyber defense program. Students learn how to identify threats and build defensible networks to minimize the impact of an attack, use tools to detect adversaries, decode and analyze packets using various tools to identify anomalies, understand how adversaries compromise networks, perform penetration testing against their own organization to find vulnerabilities, apply the six-step incident response plan, use tools to remediate malware infections, and create a data classification program to make data loss protection systems effective.

Prerequisites: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 4503: Intrusion Detection In-Depth
SANS SEC 503 | *GIAC GCIA*

ASC 4503 delivers the technical knowledge, insight, and hands-on training needed to defend networks with confidence. Students will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that they can intelligently examine network traffic for signs of an intrusion. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that students can transfer knowledge to execution.

Prerequisites: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 4508: Advanced Digital Forensics and Incident Response
SANS FOR 508 | *GIAC GCFA*
ACS 4508 teaches the necessary capabilities for forensic analysts and incident responders to identify and counter a wide range of threats within enterprise networks. This course is constantly updated and addresses today's incidents by providing hand-on forensics tactics and techniques that elite responders are successfully using in real-world breach cases.

Prerequisites: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 4510: Public Cloud Security
SANS SEC 510 | *GIAC GPCS*
ACS 4510 provides cloud security practitioners, analysts, and researchers with an in-depth understanding of the inner workings of the most popular public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Students will learn industry-renowned standards and methodologies, such as the MITRE ATT&CK Cloud Matrix and CIS Cloud Benchmarks, then apply that knowledge in hands-on exercises to assess a modern web application that leverages the cloud native offerings of each provider. Through this process students will learn the philosophies that undergird each provider and how these have influenced their services.

Prerequisites: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 4542: Web App Penetration Testing & Ethical Hacking
SANS SEC 542 | *GIAC GWAPT*
With in-depth, hands-on labs and high-quality course content, ACS 4542 helps students move beyond push-button scanning to professional, thorough, and high-value web application testing. This enables students to demonstrate the impact of inadequate security that plagues most organizations' websites. The addition of a series of enrichment exercises that strengthen students' ability to work in Python and understand how the networks and operating systems enable web attacks to succeed so as to become even more insightful penetration testers.

Prerequisites: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 4560: Network Penetration Testing & Ethical Hacking
SANS SEC 560 | *GIAC GPEN*
Every organization needs skilled information security personnel who can probe for vulnerabilities that attackers might exploit in networks, web-based applications, and computer systems, and mitigate them. ACS 4560 is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with over 30 detailed hands-on labs. After building your skills,

you'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

Prerequisites: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

Bachelor's Degree in Applied Cybersecurity Programs

The bachelor's degree in applied cybersecurity programs are designed to provide a pathway for individuals who can demonstrate a high level of aptitude for cybersecurity-related work to earn a bachelor's degree and enter the workforce.

Students in bachelor's degree programs will work towards two outcomes: (1) proficiency in the fundamental technical knowledge and skills that serve as the baseline for all professionals in cybersecurity, and (2) early specialization in advanced skills that can be applied to particular areas of information security practice.

Program Learning Outcomes

The intended learning objectives of the bachelor's degree programs are to:

- Demonstrate hands-on familiarity with the foundational technologies upon which cybersecurity excellence is built, including computer architecture, networking, programming and scripting, and Linux and Windows operating systems
- Assess cyber hygiene using the seven key Critical Security Controls and show how those specific controls enable the elements of the NIST Cybersecurity Framework
- Solve dozens of real-world cybersecurity problems in a simulated but realistic computing environment
- Assemble tools and configure systems and networks to permit them to foster resiliency and continuity of operations through attacks
- Demonstrate competence in the use of common security tools to secure Windows and Linux systems, assess vulnerabilities and exploits, and excel in the advanced area of specialization they choose.
- Demonstrate mastery of each of the learning objectives required for advanced cybersecurity courses such as those listed below.
- Write security reports and present security briefings competently
- Complete Maryland state-mandated General Education requirements

Bachelor's Degree Curriculum

The bachelor's degree in applied cybersecurity programs are a total of 120 credit hours: 50 credit hours from the SANS Technology Institute (SANS.edu) and 70 credit hours transferred from a community or 4-year college. The 50 credit hours from SANS.edu are made up of 7 required courses, 3 elective courses, and an internship. The SANS.edu curricula for the Bachelor of Professional Studies (B.P.S.) and the Bachelor of Science (B.S.) are identical. The SANS.edu curriculum should be taken in the specified order, requests to complete the curriculum in a different order should be directed to the Undergraduate Program Director.

Required Courses		**Final Exam**	**Credit Hours**
BACS 3275	Foundations: Computers, Technology, & Security	GFACT	6
BACS 3301	Introduction to Cybersecurity	GISF	4
BACS 3401	Security Essentials	GSEC	6
BACS 3402	Effective Cyber Writing and Speaking	N/A	3
BACS 3504	Security Incident Handling & Hacker Exploits	GCIH	6
BACS 3573	Automating Information Security with Python	GPYC	4
BACS 4503	Intrusion Detection In-Depth	GCIA	6
BACS 4499	Internship	N/A	6
ACS 4xxx	Elective courses (choose three)	3 GIAC exams	9

Cyber Defense

- ACS 4450: Blue Team Fundamentals: Security Operations and Analysis (GSOC)
- ACS 4487: Open-Source Intelligence (OSINT) Gathering and Analysis (GOSI)
- ACS 4501: Advanced Security Essentials (GCED)
- ACS 4505: Securing Windows and PowerShell Automation (GCWN)
- ACS 4511: Continuous Monitoring and Security Operations (GMON)

Penetration Testing

- ACS 4460: Enterprise and Cloud | Threat Vulnerability Assessment (GEVA)
- ACS 4542: Web App Penetration Testing and Ethical Hacking (GWAPT)
- ACS 4560: Network Penetration Testing and Ethical Hacking (GPEN)
- ACS 4575: Mobile Device Security and Ethical Hacking (GMOB)

Security Management

- ACS 4566: Implementing and Auditing the Critical Security Controls In-Depth (GCCC)

Digital Forensics and Incident Response

- ACS 4498: Battlefield Forensics & Data Acquisition (GBFA)
- ACS 4500: Windows Forensic Analysis (GCFE)
- ACS 4508: Advanced Incident Response, Threat Hunting, and Digital Forensics (GCFA)

Cloud Security

- ACS 4488: Cloud Security Essentials (GCLD)
- ACS 4510: Public Cloud Security (GPCS)
- ACS 4522: Defending Web Applications Security Essentials (GWEB)
- ACS 4540: Cloud Security and DevOps Automation (GCSA)
- ACS 4588: Cloud Penetration Testing (GCPN)

Industrial Control Systems Security

- ACS 4410: ICS/SCADA Security Essentials (GICSP)

Course Listings and Descriptions

BACS 3275: Foundations: Computers, Technology, & Security
SANS SEC 275 | Supplemental Materials | GIAC GFACT
BACS 3275 is purpose-built to provide students with the fundamental technical knowledge and skills that serve as the baseline for all professionals in cybersecurity, reinforcing key concepts with interactive labs. You'll establish a core understanding of technology component functions and apply that knowledge to security concepts such as reconstructing a crime from digital evidence or locating exploitable flaws in software and websites. The course ensures a solid mastery of computer, hardware, network, and cybersecurity fundamentals, including the study of operating systems, Windows security tools, Linux, programming with Python and C, advanced Google searches, reconnaissance, virtualization, and encryption. You'll explore the inner workings of packets and protocols that allow the internet to function and learn the role of a computer's central processing unit (CPU), how it executes code, its relationship with memory, and the fundamentals of how attackers disrupt intended behavior.

6 Credit Hours | 8 Week Course Term
* This course was previously numbered BACS 3201

BACS 3301: Introduction to Cybersecurity
SANS SEC 301 | Supplmental Materials | GIAC GISF
BACS 3301 instills familiarity with core security terms and principles. This course covers everything from core terminology to the how computers and networks function, security policies, risk management, a new way of looking at passwords, cryptographic principles, network attacks & malware, wireless security, firewalls and many other security technologies, web & browser security, backups, virtual machines & cloud computing.

Prerequisites: BACS 3275
4 Credit Hours | 8 Week Course Term
*Note: this course can be taken concurrently with BACS 3402

BACS 3401: Security Essentials
SANS SEC 401 | Supplmental Materials | GIAC GSEC
BACS 3401 is a technically-oriented survey course in which you'll learn the most effective steps to prevent cyber attacks and detect adversaries. In classes and hands-on labs, you'll learn to develop effective security metrics that provide a focused playbook that IT can implement, auditors can validate, and executives can understand. You'll explore methods to analyze and assess the risk to your environment in order to drive the creation of a security roadmap that focuses on the right areas of security. And you'll learn practical tips and tricks to focus in on high-priority security problems and on the actions required to protect and secure an organization's critical information assets and business systems.

Prerequisites: BACS 3301, BACS 3402
6 Credit Hours | 8 Week Course Term

BACS 3402: Effective Cyber Writing and Speaking
SANS SEC 402 & SEC 403 | Supplemental Materials | No GIAC exam
This unique course, built exclusively for those in cybersecurity, will strengthen your writing and speaking skills. During the first half of the course, you will learn the five "golden elements" of effective reports, briefings, emails, and other cybersecurity writing as well as understand how to

pick the best words, structure, look, and tone. The second half of the course gives you the skills to put together an effective security briefing, secure the interest and engagement of your audience, and confidently deliver presentations to a variety of groups.

Prerequisites: BACS 3275
3 Credit Hours | 8 Week Course Term
*Note: this course can be taken concurrently with BACS 3301

BACS 3504: Security Incident Handling and Hacker Exploits

SANS SEC 504 | *Supplemental Materials* | *GIAC GCIH*

BACS 3504 is 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 today.

Prerequisites: BACS 3401
6 Credit Hours | 8 Week Course Term

BACS 3573: Automating Information Security with Python

SANS SEC 573 | *Additional Labs* | *GIAC GPYC*

This 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.

Prerequisites: BACS 3504
4 Credit Hours | 8 Week Course Term
*Note: this course can be taken concurrently with an elective course in the program

BACS 4503: Intrusion Detection In-Depth

SANS SEC 503 | *Supplemental Materials* | *GIAC GCIA*

BACS 4503 delivers the technical knowledge, insight, and hands-on training needed to defend networks with confidence. Students will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that they can intelligently examine network traffic for signs of an intrusion. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that students can transfer knowledge to execution.

Prerequisites: BACS 3504
6 Credit Hours | 8 Week Course Term

BACS 4499: Internet Storm Center (ISC) Internship
Much like the World Health Organization and its global disease monitoring network, the SANS Technology Institute, through its research wing in the Internet Storm Center (ISC), maintains and operates the world's leading global cyber threat detection network.

The ISC depends on continuous input from a series of DShield sensors and web application honeypots. Of course, all that collected data accomplishes nothing if it is not processed, interpreted, analyzed and very quickly reported to the global information security community. This is the role of the ISC handlers, the frontline personnel of global threat detection, whose main task is to take all the input received into the ISC and turn it into "diaries" (https://isc.sans.edu/diaryarchive.html).

This internship as an Apprentice Handler will provide a student with a continuous opportunity over the course of 20 weeks to observe emerging threats, to analyze and report upon those threats, and to gain experience under the mentorship of a Handler or Senior Handler. This hands-on, real-world experience will prepare the student for a first professional cybersecurity role in a way that few other programs can. That experience will include not only a deepening of practical understanding of real-world technical issues, but also the ability to effectively write and communicate about those issues.

Prerequisites: BACS 3504
6 Credit Hours | 20 Week Course Term
*Note: this internship can be taken concurrently with the elective courses in the program

Technical Elective Course Options

ACS 4410: Security Essentials for Industrial Control Systems
SANS ICS 410 | GIAC GICSP
ACS 4410 is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. Students will learn the language, the underlying theory, and the basic tools for industrial control system security in setting across a wide range of industry sectors and applications.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4450: Blue Team Fundamentals: Security Operations and Analysis
SANS SEC 450 | GIAC GSOC
ACS 4450 provides students with technical knowledge and key concepts essential for security operation center (SOC) analysts and new cyber defense team members. By providing a detailed explanation of the mission and mindset of a modern cyber defense operation, this course will jumpstart and empower those on their way to becoming the next generation of blue team members.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4460: Enterprise and Cloud | Threat & Vulnerability Assessment
SANS SEC 460 | GIAC GEVA
ACS 4460 covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous

defensive strategy from day one. The course focuses on equipping information security personnel from mid-sized to large organizations who are charged with effectively and efficiently securing 10,000 or more systems.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4487: Open-Source Intelligence (OSINT) Gathering and Analysis
SANS SEC 487 | GIAC GOSI
ACS 4487 is a foundational course in open-source intelligence (OSINT) gathering that teaches students real-world skills and techniques that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amounts of information found on the Internet. Once the information is gathered, this course will show you how to ensure that it is corroborated, how to analyze what you've gathered, and how to make sure it is useful in your investigations.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4488: Cloud Security Essentials
SANS SEC 488 | GIAC GCLD
ACS 4488 covers Amazon Web Services, Azure, Google Cloud, and other cloud service providers (CSPs). Like foreign languages, cloud environments have similarities and differences, and this course will introduce you to the language of cloud security. Upon completion of this course, you will be able to advise and speak about a wide range of cybersecurity topics and successfully navigate the challenges and opportunities presented by cloud service providers.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4498: Battlefield Forensics & Data Acquisition
SANS FOR 498 | GIAC GBFA
This course provides the necessary skills to identify the many and varied data storage mediums in use today and how to collect and preserve this data in a forensically sound manner despite how and where it may be stored. It covers digital acquisition from computers, portable devices, networks, and the cloud. It then teaches the student Battlefield Forensics, or the art and science of identifying and starting to extract actionable intelligence from a hard drive in 90 minutes or less.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4500: Windows Forensic Analysis
SANS FOR 500 | GIAC GCFE
This course 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.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4501: Advanced Enterprise Defender

SANS SEC 501 | *GIAC GCED*

ACS 4501 brings together all the elements of a modern cyber defense program. Students learn how to identify threats and build defensible networks to minimize the impact of an attack, use tools to detect adversaries, decode and analyze packets using various tools to identify anomalies, understand how adversaries compromise networks, perform penetration testing against their own organization to find vulnerabilities, apply the six-step incident response plan, use tools to remediate malware infections, and create a data classification program to make data loss protection systems effective.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4505: Securing Windows and PowerShell Automation

SANS SEC 505 | *GIAC GCWN*

ACS 4505 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.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4508: Advanced Digital Forensics and Incident Response

SANS FOR 508 | *GIAC GCFA*

ACS 4508 teaches the necessary capabilities for forensic analysts and incident responders to identify and counter a wide range of threats within enterprise networks. This course is constantly updated and addresses today's incidents by providing hand-on forensics tactics and techniques that elite responders are successfully using in real-world breach cases.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4510: Public Cloud Security

SANS SEC 510 | *GIAC GPCS*

ACS 4510 provides cloud security practitioners, analysts, and researchers with an in-depth understanding of the inner workings of the most popular public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Students will learn industry-renowned standards and methodologies, such as the MITRE ATT&CK Cloud Matrix and CIS Cloud Benchmarks, then apply that knowledge in hands-on exercises to assess a modern web application that leverages the cloud native offerings of each provider. Through this process students will learn the philosophies that undergird each provider and how these have influenced their services.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4511: Continuous Monitoring and Security Operations
SANS SEC 511 | GIAC GMON
A new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses. ACS 4511 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.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4522: Defending Web Applications Security Essentials
SANS SEC 522 | GIAC GWEB
This course 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.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4540: Cloud Security and DevOps Automation
SANS SEC 540 | GIAC GCSA
This course provides security professionals with a methodology for securing modern Cloud and DevOps environments. Students learn how to implement over 20 DevSecOps Security Controls for building, testing, deploying, and monitoring cloud infrastructure and services. Immersive hands-on labs ensure students not only understand theory, but how to configure and implement each security control. By embracing the DevOps culture, students will walk away battle tested and ready to build an organization's Cloud & DevOps Security program.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4542: Web App Penetration Testing & Ethical Hacking
SANS SEC 542 | GIAC GWAPT
With in-depth, hands-on labs and high-quality course content, ACS 4542 helps students move beyond push-button scanning to professional, thorough, and high-value web application testing. This enables students to demonstrate the impact of inadequate security that plagues most organizations' websites. The addition of a series of enrichment exercises that strengthen students' ability to work in Python and understand how the networks and operating systems enable web attacks to succeed so as to become even more insightful penetration testers.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4560: Network Penetration Testing & Ethical Hacking
SANS SEC 560 | GIAC GPEN

Every organization needs skilled information security personnel who can probe for vulnerabilities that attackers might exploit in networks, web-based applications, and computer systems, and mitigate them. ACS 4560 is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with over 30 detailed hands-on labs. After building your skills, you'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4566: Implementing and Auditing the Critical Security Controls In-Depth
SANS SEC 566 | GIAC GCCC
Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. ACS 4566 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.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4575: Mobile Device Security and Ethical Hacking
SANS SEC 575 | GIAC GMOB
ACS 4575 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.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

ACS 4588: Cloud Penetration Testing
SANS SEC 588 | GIAC GCPN
ACS 4588 equips you with the latest in cloud-focused penetration testing techniques and teaches you how to assess cloud environments. The course dives into topics like cloud-based microservices, in-memory data stores, serverless functions, Kubernetes meshes, and containers, as well as identifying and testing in cloud-first and cloud-native applications. You will also learn specific tactics for penetration testing in Azure and Amazon Web Services, particularly important given that AWS and Microsoft account for more than half the market.

Prerequisites: BACS 3504
3 Credit Hours | 8 Week Course Term

Admissions Requirements and Application Process

All applicants must meet the following criteria:

- Be at least 18 years old (or will be at the time of enrollment)

Applicants for the undergraduate certificate program must meet the following criteria:

- Have completed at least 48 college credits from a recognized college or university
- A cumulative GPA (grade point average) of 2.80 or greater

Applicants for the Bachelor of Science (B.S.) program must meet the following criteria:

- Have completed at least 60 college credits from a recognized college or university
- A GPA of 3.0 or greater

Applicants for the Bachelor of Professional Studies (B.P.S.) program must meet the following criteria:

- Be enrolled in or have completed an A.A.S. degree program
- A GPA of 3.0 or greater at completion of the A.A.S. degree program

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

a) Application Form
b) Current Resume (optional)
c) Official Transcripts
d) Aptitude Assessment
e) Application Fee
f) Requirements for International Students (if applicable)
    a. Transcript evaluation through World Evaluation Services (WES), or similar service.
    b. Non-native English speakers must submit TOEFL/IELTS scores.

Application Submission

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

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 45 minutes to complete the orientation modules and survey and an additional 30-60 minutes for the academic advising appointment (30 minutes for the certificate program and 60 minutes for a bachelor's program). For details on the start dates and preferred deadlines, please visit https://www.sans.edu/admissions/orientation.

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.

Undergraduate students pay a flat tuition rate per course. All course materials are included in the cost of tuition and are provided to the student directly. Students taking courses online (using SANS OnDemand) 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 undergraduate course tuition.

Certificate Program in Applied Cybersecurity

The table below reflects tuition rates for the Applied Cybersecurity Certificate Program.

Course	Course Cost	Credits
ACS 3275	$1,375	3
ACS 3401	$5,500	3
ACS 3504	$5,500	3
ACS Elective	$5,500	3
Applied Cybersecurity (ACS) Program Total	***$17,875***	***12***

Bachelor's Degree Programs in Applied Cybersecurity

The table below reflects tuition rates for the Applied Cybersecurity Bachelor's Programs.

Course	Course Cost	Credits
BACS 3275	$1,375	6
BACS 3301	$4,125	4
BACS 3401	$4,125	6
BACS 3402	$1,375	3
BACS 3504	$4,125	6
BACS 3573	$4,125	4
BACS 3503	$4,125	6
ACS Elective	$4,125	3
ACS Elective	$4,125	3
ACS Elective	$4,125	3
BACS 4499	$0	6
Bachelor's Degree in Applied Cybersecurity Program Total	***$35,750***	***50***

Fees

The following fees may apply:

Application Fee*	$35
Course Change Fee	$150
Cancellation Fee	$300
GFACT Exam Retake Fee	$200
GIAC Exam Retake Fee	$799

* Paid during the application process

Cost of Live Learning Events

Travel and Lodging

Students are responsible for the costs of hotel, food, and travel should they choose to 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 undergraduate 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.

Income Share Agreement ("ISA")

ISA Basics

An Income Share Agreement ("ISA") is a legal contract between a student and the SANS Technology Institute. For students who qualify and are accepted to this funding program, the ISA contract outlines that in exchange for the provision of an education to the student, said student agrees to pay a fixed percentage of their gross income (i.e. before taxes) for a fixed duration of time upon their completion of the program of study. Upon departure from the program, payment of the ISA occurs when the student is employed and earning above the predetermined minimum income threshold. Leif (Leif.org) is contracted as the ISA Program Manager, and as such, Leif will support ISA students with ISA enrollment, contract management and support, and financial reporting and repayment requirements. Students should manage all financial requirements of their ISA contract, including income reporting and repayment, through the Leif online portal (Leif.org).

The following are key concepts and terms that will be defined in a student's ISA contract:

- An ISA is a legally binding agreement representing a responsibility to pay SANS Technology Institute a portion of future income for the education provided.
- Income Share Agreements are not a form of debt, nor are they a loan. They have no interest rate or principal balance.
- Payment Cap: the maximum amount a student can be required to pay to satisfy the contract
- Income Share %: the percentage of gross future income a student agrees to pay on the contract monthly once the minimum income threshold is met
- Minimum Income Threshold: the minimum gross income a student must earn to trigger repayment of the contract
- Payment Term: the maximum number of monthly payments required to satisfy the contract
- Deferment Period: the maximum number of months below the minimum income threshold allowed before the contract is cancelled
- A student will satisfy the ISA contract by reaching **one** of the following milestones: reach the payment cap, reach the payment term, or reach the end of the deferment period

The ISA Terms will be agreed upon between the student and SANS Technology Institute during the application process. As such, any other costs that a student may incur during their time in the undergraduate program cannot be covered by the ISA. Below are situations that a student may be required to pay the SANS Technology Institute during their time in the program.

- Exam or course retake fees
- Course cancellation or change fees
- Other fees or costs not associated with the basic tuition of the program
- Any travel and lodging expenses related to attending a Live course

Although career services are provided by the SANS Technology Institute, the school cannot guarantee a job to any student or graduate.

ISA Withdrawal or Dismissal Refund Policy

Should a student under ISA contract with SANS Technology Institute withdraw or be dismissed from the undergraduate program of study, they will be eligible to reduce their ISA payment cap obligation according to their progress through the enrolled program of study. Upon departure from the program, the ISA payment cap will be refunded the cumulative amount of all courses for which

course registration has not been processed (see **Appendix A** for the payment cap impact of each course). No other part of the departing student's ISA contract will be adjusted, and the student agrees to pay the new payment cap within all of the other contractual agreements and protections of the original ISA contract. For clarity, registrations are processed 7-10 days prior to the actual start date of the course. There is no refund for a course after a course registration is processed as this processing provides a student with all underlying SANS curriculum resources and the GIAC certification resources and attempts. Although no longer a part of the program, after departure from a SANS Technology Institute undergraduate program a student whose registration was processed could still choose to complete the SANS curriculum and attempt and earn the GIAC certification. *See **Appendix A** for ISA contract refund amounts and examples.*

Cyber FastTrack Scholarship

The Cyber FastTrack (CFT) scholarship can be used towards tuition for the Applied Cybersecurity certificate program. The amount of tuition covered by the scholarship is provided at the time the scholarship is awarded. As such, any other costs that a student may incur during their time in the undergraduate program cannot be covered by the scholarship. Below are situations that a student may be required to pay SANS.edu during their time in the program.

- Tuition not covered by a partial scholarship
- Exam or course retake fees
- Course cancellation or change fees
- Other fees or costs not associated with the basic tuition of the program
- Any travel and lodging expenses related to attending a Live course

Cyber FastTrack Academic Standard

CFT scholarship recipients are expected to maintain the highest standards of academic effort and excellence while working through the Applied Cybersecurity certificate program. As such, to maintain the CFT scholarship, recipients must earn a final grade of B or higher in each course. Earning below a final grade of a B in a course will result in the immediate loss of the scholarship. Students who lose the scholarship by failing to meet this higher academic standard can still continue in the program, but they will be responsible for the tuition requirements of any remaining courses.

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 by the VA. Please refer to the Veterans Benefits section towards the end of this catalog for more detailed information.

Cancellation and Change Fees

Students who wish to cancel and receive a refund for a particular 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 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.

Credit Transfers and Waivers

Credit Transfers

The SANS Technology Institute does not accept transfers of credit for coursework completed at other higher education institutions.

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 an undergraduate course to complete both a relevant SANS Institute class and GIAC exam if the student has sat for and 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.

CISSP Certification

For students who hold a current CISSP from the ISC^2 organization, a waiver will be granted within ACS 3401 and BACS 3401 for the SANS class SEC 401. Achievement of the associated GIAC GSEC exam will still be required for the award of credit. Students pursuing this option will register and pay tuition for the GIAC GSEC exam but will *not* receive course materials for the SANS SEC 401 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.)

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.

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:
Hyatt Regency Baltimore
300 Light Street
Baltimore, MD 21201

Hilton Baltimore
401 W Pratt Street
Baltimore, MD 21201

Columbia:
Sheraton Columbia Town Center
10207 Wincopin Circle
Columbia, MD 21044 US

Bethesda:
Hyatt Regency Bethesda
One Bethesda Metro Center
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®: Benefits, Tuition, and Fees

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 is the deadline for any schedule changes.

- Bachelor's students using GI Bill® will have a full-time 'rate of pursuit' if at least 6 credits are pursued during an 8 week term.
- Undergraduate certificate students using GI Bill® will have a 'rate of pursuit' greater than half-time in each term (course) if the ACS accelerated version of courses is pursued.
- 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 but we will not adjust the certification as the course term remains the same.

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 student's rate of pursuit.

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, 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:
Students are responsible for any costs not covered by the VA. Situations in which a student using GI Bill® benefits may owe out-of-pocket tuition include, but are not limited to:

- Student is less than 100% eligible for benefits
- Student's certifications exceed the annual private school tuition cap
- Student withdraws from a course that was certified to the VA
- Student stops meeting attendance requirements in a course that was certified to the VA

Tuition balances not paid by the due date may be sent to collections and incur additional fees up to 35% of the balance due.

Please note:

- Student Veterans will not be penalized while the college awaits payment from the Department of Veteran Affairs.
- 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 Technology Institute (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.

  (1) 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.
  (2) 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 vLive or Simulcast modalities, and on the 1st or 15th of the month for OnDemand courses.

Please note refunds are not given after classes begin for in-person/vLive courses and 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. SANS.edu 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.edu 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

Appendices

Appendix A: ISA Contract Refund Tables and Examples

The tables and examples below describe the ISA contract refund amounts that apply to ACS and BACS ISA contracts.

Certificate in Applied Cybersecurity ISA Contract Refund Table and Examples

ACS Course	Payment Cap Impact per Course
ACS 3275	$1600.00
ACS 3401	$6300.00
ACS 3504	$6300.00
ACS 4XXX (elective)	$6300.00
Total for full program	*$20,500.00*

Table A. Payment Cap Impact Per ACS Course

A couple of ACS refund examples:

- Student A, who fully-funded the ACS program tuition with an ISA, agreed to a payment cap of $20,500 (see Table A). If Student A leaves the ACS program after registration is processed for ACS 3275, then Student A's ISA contract will be adjusted to show a payment cap refund of $18,900 resulting in a new payment cap of $1600. Effectively Student A is still responsible for the $1600 cost of tuition for ACS 3275, but will not be paying for the tuition for ACS 3401, ACS 3504 and ACS 4XXX (elective) for which the student did not receive any resources, materials, instruction, or certification attempts.
- Student B, who also fully-funded the ACS program tuition with an ISA, agreed to a payment cap of $20,500 (see Table A). If Student B leaves the ACS program after completing ACS 3275 and registration is processed for ACS 3401, then Student B's ISA contract will be adjusted to show a payment cap refund of $12,600 resulting in a new payment cap of $7,900. Effectively Student B is still responsible for the cost of tuition for ACS 3275 and ACS 3401, but will not be paying for the tuition for ACS 3504 and ACS 4XXX (elective) for which the student did not receive any resources, materials, instruction, or certification attempts.

Bachelor's Degree in Applied Cybersecurity ISA Contract Refund Table and Examples

BACS Course	Payment Cap Impact per Course
BACS 3275	$1600.00
BACS 3301	$4700.00
BACS 3402	$1600.00
BACS 3401	$4700.00
BACS 3504	$4700.00
BACS 3573	$4700.00
BACS 4503	$4700.00
ACS 4XXX (elective)	$4700.00
ACS 4XXX (elective)	$4700.00
ACS 4XXX (elective)	$4700.00
BACS 4499	$0
Total for full program	*$40,800.00*

Table B. Payment Cap Impact Per BACS Course

A couple of bachelor's degree (BACS) refund examples:

- Student C, who fully-funded the program tuition with an ISA, agreed to a payment cap of $40,800 (see Table B). If Student C leaves the BACS program after registration is processed for BACS 3275, then Student C's ISA contract will be adjusted to show a payment cap refund of $39,200 resulting in a new payment cap of $1600. Effectively Student C is still responsible for the $1600 cost of tuition for BACS 3275, but will not be paying for the tuition for any of the remaining courses in the BACS program for which the student did not receive any resources, materials, instruction, or certification attempts.
- Student D, who also fully-funded the ACS program tuition with an ISA, agreed to a payment cap of $40,800 (see Table B). If Student D leaves the BACS program after completing BACS 3275, BACS 3301, and BACS 3402, and registration is processed for BACS 3401, then Student D's ISA contract will be adjusted to show a payment cap refund of $28,200 resulting in a new payment cap of $12,600. Effectively Student D is still responsible for the $12,600 cost of tuition for BACS 3275, BACS 3301, BACS 3402, and BACS 3401, but will not be paying for the tuition for any of the remaining courses in the BACS program for which the student did not receive any resources, materials, instruction, or certification attempts.