SANS Technology Institute

2026 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 *5*
2026 Select Live Learning Event Schedule 5
Cybersecurity Fundamentals Certificate Program *6*
Program Learning Outcomes **6**
CSF Curriculum **6**
Satisfactory Academic Progress **6**
Funding Restrictions **7**
Course Listings and Descriptions **7**
Applied Cybersecurity Certificate Program *8*
Program Learning Outcomes **8**
ACS Curriculum **8**
Course Listings and Descriptions **9**
Technical Elective Course Options 10
Bachelor's Degree in Applied Cybersecurity Program *14*
Program Learning Outcomes **14**
Bachelor's Degree Curriculum **15**
Required Courses 15
BACS Technical Elective Course Options 16
Course Listings and Descriptions **17**
Block 1 17
Block 2 19
Technical Elective Course Options 21
Credit Hours *26*
Admissions Requirements and Application Process *26*
Application Submission 27
Invitation to Matriculate 27
New Student Orientation 27
Registration *28*
Course Registration Deadline 28
Course Start Dates by Modality 28
Add/Drop Policy 28
Tuition and Fees *29*
Certificate Program in Cybersecurity Fundamentals **29**
Certificate Program in Applied Cybersecurity **29**
Bachelor's Degree Programs in Applied Cybersecurity **29**
Single Courses, Non-degree Seeking Students **30**
Fees **30**

Cost of Live Learning Events **31**
Travel and Lodging 31
Live Class Add-ons 31
Cancellation and Change Fees **31**
Financial Aid/Title IV Eligibility **32**
SANS.edu Step Up Payment Plan (SUPP) **32**
Step Up Payment Plan Basics 32
Step Up Payment Plan Policies 33
SANS.edu Tuition Payment Program (TPP) **35**
TPP Basics 35
TPP Policies 36
Veterans Benefits **38**
Credit Transfers and Waivers ***38***
Credit Transfers **38**
Undergraduate Programs Transfer Credit 38
Technology and Software Requirements ***40***
Suggested Laptop Requirements **40**
Laptop Requirements 40
Operating System 41
Technology Requirements for the ISC Internship (BACS 4499) **41**
DShield Honeypot Basics 41
Veterans Benefits ***42***
Introduction **42**
Background Information **42**
Approved Live Learning Events for 2025 ..... **43**
Baltimore: 43
Columbia: 43
Rockville: 43
Bethesda: 43
Chapter 33 Post-9/11 GI Bill® **43**
Costs Covered 43
Rate of Pursuit 44
Housing Allowance 44
Books and Fees Stipend 45
Vocational Rehabilitation & Employment **45**
Costs Covered 45
Other GI Bill® Chapters, including Chapter 30 Montgomery Bill **45**
Costs Covered 45
Yellow Ribbon Program **46**
Registering and Paying for Courses **46**
Tuition & Fees 46
VA Requirements of GI Bill® Users **47**

Course Attendance Requirements 47
VA Requirements of SANS Technology Institute 48
What students can expect from the VA 48
VA Resources and Contact Information 49
California State Tuition Recovery Fund Disclosures 50
Course Catalog Archive 52

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 course students are enrolled in. Though students enjoy this flexible enrollment model, student progress and enrollment reporting are 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.

Our offices are closed on: New Year's Day, Martin Luther King Jr Day, Memorial Day, Juneteenth Day, Independence Day, Labor Day, Thanksgiving and the day 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.

2026 Select Live Learning Event Schedule

Event*	Start Date
Spring Semester Cycle	
SANS Rockville 2026	February, 2026
SANS Orlando 2026	March-April 2026
SANS Security West	May, 2026
SANS Orlando 2026	March-April, 2026
SANS Chicago 2026	June, 2026
Fall Semester Cycle	
SANSFIRE 2026	July, 2026
SANS Virginia Beach 2026	August-September, 2026
SANS Network Security 2026	September, 2026
SANS Cyber Defense Initiative 2026	December, 2026

*Events are subject to change. The full schedule of upcoming events is available online at: https://www.sans.org/cyber-security-events

Cybersecurity Fundamentals Certificate Program

The Lower Division Undergraduate Certificate in Cybersecurity Fundamentals (CSF) program is designed to provide students with a powerful and effective introduction to the fundamental skills and knowledge needed to succeed in both our upper division undergraduate certificate and bachelor's degree programs in applied cybersecurity.

Students in the CSF program will work towards gaining mastery and confidence in foundational concepts underlying the best cybersecurity practitioners including mathematics, coding, technology components and systems, and core cybersecurity skills and concepts.

Program Learning Outcomes

The intended learning objectives of the CSF program are to:

- Distill some of the most important mathematics foundations that apply to computer science and information security.
- Teach basic Python coding skills in Windows and Linux environments.
- Ensure a level of sufficient theoretical understanding and applied practical skills that will enable the student to speak the same language as industry professionals.

CSF Curriculum

The Lower Division Undergraduate Certificate program in Cybersecurity Fundamentals (CSF) is a total of 12 credit hours and is made up of three (3) courses. Courses must be taken in the order shown below.

Required Courses		**GIAC Exam**	**Credit Hours**
CSF 2395	Applied Mathematics for Information Security Professionals	N/A	3
CSF 2373	Introductory Python	N/A	3
CSF 2275	Foundations: Computers, Technology, & Security	GFACT	6

Satisfactory Academic Progress

Students in the Cybersecurity Fundamentals undergraduate certificate program must pass their first and second course, CSF 2395 and CSF 2373, on the first attempt in order to remain in the program. Failure to pass either courses will result in dismissal from the program. Students who do not pass the final course, CSF 2275, on the first attempt will be put on academic probation and allowed to retake the course one time only. See the Student Handbook for more information on Satisfactory Academic Progress.

Funding Restrictions

This program is not eligible for the SANS.edu Tuition Payment Plan (TPP) programs.

Course Listings and Descriptions

CSF 2395: Applied Mathematics for Information Security Professionals

CSF 2395 covers the most important mathematics foundations that apply to computer science and information security, namely the fundamentals of cryptography and the notions of sets and closed systems. At the conclusion of this course, students will be able to reason on and apply fundamental mathematics as they interface with computer science and cybersecurity topics.

Prerequisites: None
3 Credit Hours | Course Length: 13 weeks

CSF 2373: Introductory Python

CSF 2373 is a hands-on course that teaches students by having them actively write Python code so that they can see successful results and learn by doing. Using that practical approach, this course teaches students how to install and maintain Python programs and modules and to utilize basic Python programming concepts such as functions, IDEs, modules, lists, and basic file input/output.

Prerequisites: CSF 2395
3 Credit Hours | Course Length: 13 weeks

CSF 2275: Foundations: Computers, Technology, & Security
SANS SEC275 | GIAC GFACT

CSF 2275 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. Students 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. Students 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.

Prerequisites: CSF 2395 and CSF 2373
6 Credit Hours | Course Length: 13 weeks

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. Courses must be taken in the order shown below.

Required Courses		**GIAC 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

ACS Technical Elective Course Options

Cyber Defense
- ACS 4450: Blue Team Fundamentals: Security Operations and Analysis (GSOC)
- ACS 4501: Advanced Security Essentials (GCED)
- ACS 4503: Network Monitoring and Threat Detection In-Depth (GCIA)
- ACS 4511: Continuous Monitoring and Security Operations (GMON)

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

Digital Forensics and Incident Response
- ACS 4500: Windows Forensic Analysis (GCFE)
- ACS 4508: Advanced Incident Response, Threat Hunting, and Digital Forensics (GCFA)

Cloud Security
- ACS 4502: Cloud Security Tactical Defense (GCLD)
- ACS 4510: Public Cloud Security: AWS, Azure, and GCP (GPCS)

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

Course Listings and Descriptions

ACS 3275: Foundations: Computers, Technology, & Security
SANS SEC275 | *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. Students 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. Students 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.

Prerequisites: None
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 3401: Security Essentials
SANS SEC401 | *GIAC GSEC*

ACS 3401 is a technically-oriented survey course in which students learn the most effective steps to prevent cyber attacks and detect adversaries. In classes and hands-on labs, students learn the essential information security skills and techniques needed to protect and secure critical information and technology assets, whether on-premise or in the cloud. Student will also learn how to directly apply the concepts learned in developing a winning defensive strategy, all in the terms of the modern adversary.

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

ACS 3504: Hacker Tools, Techniques, and Incident Handling
SANS SEC504 | *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: ICS/SCADA Security Essentials
SANS ICS410 | *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 SEC450 | *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 4500: Windows Forensic Analysis

SANS FOR500 | *GIAC GCFE*

ACS 4500 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: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 4501: Advanced Enterprise Defender
SANS SEC501 | *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 4502: Cloud Security Tactical Defense
SANS SEC502 | *GIAC GCLD*

ACS 4502 equips practitioners with advanced, hands-on experience to secure modern cloud environments against evolving threats. Through live labs in real cloud environments, students will design and enforce tactical controls across identity, data, and network layers, addressing real-world risks like misconfigurations, privilege escalation, credential theft, data theft, and lateral movement. With 40 immersive, live-fire labs and a competitive Capture the Flag challenge, participants gain the expertise to harden cloud infrastructure, lead incident response efforts, and implement security strategies aligned with enterprise-scale deployments and compliance frameworks.

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

ACS 4503: Network Monitoring and Threat Detection In-Depth
SANS SEC503 | *GIAC GCIA*

ACS 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, Incident Response, & Threat Hunting
SANS FOR508 | *GIAC GCFA*

ACS 4508 teaches students 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: AWS, Azure, and GCP
SANS SEC510 | *GIAC GPCS*

ACS 4510 provides students 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 4511: Continuous Monitoring and Security Operations
SANS SEC511 | *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: ACS 3504
3 Credit Hours | Course Length: Standard (13 weeks) or Accelerated (8 weeks)

ACS 4542: Web App Penetration Testing & Ethical Hacking
SANS SEC542 | *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: Enterprise Penetration Testing
SANS SEC560 | *GIAC GPEN*

Both the offensive teams and defenders of an enterprise have the same goal: keep the real bad guys out. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specifically developed to get students ready for that role. ACS 4560 is designed to strengthen penetration testers and further add to their skillset. The course is also designed to train system administrators, defenders, and others in security to understand the mindset and methodology of a modern attacker. Students will learn how to plan, prepare, and execute a penetration test in a modern enterprise. Using the latest penetration testing tools, students will undertake extensive hands-on lab exercises to learn the methodology of experienced attackers and practice their skills.

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

Bachelor's Degree in Applied Cybersecurity Program

The bachelor's degree in applied cybersecurity is 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 the bachelor's degree program will work towards two overall 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

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

1. Mastery of Foundational Cybersecurity Technologies
   - 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.
   - Assemble tools and configure systems and networks to foster resiliency and continuity of operations through attacks.

2. Competence in Security Tools and Techniques
   - Demonstrate competence in the use of common security tools to secure all modern operating systems and platforms, assess vulnerabilities and exploits, and excel in the advanced area of specialization they choose.
   - Solve real-world cybersecurity problems in simulated but realistic computing environments.

3. Cyber Hygiene and Framework Implementation
   - Assess cyber hygiene using the seven key Critical Security Controls.
   - Show how those specific controls enable a range of Cybersecurity Frameworks, including NIST.

4. Effective Communication and Reporting
   - Communicate security issues effectively to a range of technical and non-technical stakeholders.
   - Write security reports and present security briefings competently.

5. Professional Development and Networking
   - Start to build a professional network across the information security community.
   - Develop a portfolio to showcase cybersecurity achievements and projects.

Bachelor's Degree Curriculum

The bachelor's degree in applied cybersecurity program is 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 8 required courses, 3 elective courses, 2 Portfolio Practicum requirements, and a Field Experience Practicum. 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 Dean of Students Office.

Required Courses

Course		GIAC Exam	Credit Hours
BLOCK 1 (courses must be taken in the specified order)			
BACS 3275	Foundations: Computers, Technology & Security	GFACT	6
BACS 3001	*Portfolio Practicum* Experiential Learning Through Cyber Challenges (Foundational)		3
BACS 3401	Security Essentials	GSEC	4
BACS 3504	Hacker Tools, Techniques, and Incident Handling	GCIH	4
BACS 3402	Effective Cyber Writing and Speaking	N/A	2
BACS 3373	Introductory Python	N/A	3
BACS 3573	AI-Powered Security Automation: Building Tools with Python, LLMs and MCP	GPYC	4
		Block 1 Total	***26***
BLOCK 2 (courses can be taken in any order)			
BACS 4499 / BACS 4001	*Field Experience Practicum* Choose one option: BACS 4499 - ISC Internship BACS 4001 - External Internship		4

BACS 3500	Windows Forensic Analysis	GCFE	4
BACS 3503	Network Monitoring and Threat Detection In-Depth	GCIA	4
ACS _ _ _ _	Elective Courses (choose 3)	3 GIAC exams	9
BACS 3002	*Portfolio Practicum* Experiential Learning Through Cyber Challenges (Advanced)		3
		Block 2 Total	***24***
		Program Total	**50**

BACS Technical Elective Course Options

Cyber Defense

- ACS 4450: Blue Team Fundamentals: Security Operations and Analysis (GSOC)
- ACS 4497: Practical Open-Source Intelligence (OSINT) (GOSI)
- ACS 4501: Advanced Security Essentials (GCED)
- ACS 4511: Continuous Monitoring and Security Operations (GMON)
- ACS 4595: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals (GMLE)

Penetration Testing

- ACS 4542: Web App Penetration Testing and Ethical Hacking (GWAPT)
- ACS 4560: Enterprise Penetration Testing (GPEN)
- ACS 4575: Mobile Device Security and Ethical Hacking (GMOB)

Security Leadership

- ACS 4566: Implementing & Auditing the Critical Security Controls (GCCC)

Digital Forensics and Incident Response

- ACS 4498: Digital Acquisition and Rapid Triage (GBFA)
- ACS 4508: Advanced Incident Response, Threat Hunting, and Digital Forensics (GCFA)
- ACS 4577: Linux Incident Response and Threat Hunting (GLIR)

Cloud Security

- ACS 4502: Cloud Security Essentials (GCLD)
- ACS 4510: Public Cloud Security: AWS, Azure, and GCP (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)
- ACS 4456: Essentials for NERC Critical Infrastructure Protection (GCIP)
- ACS 4515: ICS Visibility, Detection, and Response (GRID)

Course Listings and Descriptions

Block 1

BACS 3275: Foundations: Computers, Technology, & Security
SANS SEC275 | *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. Students 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. Students 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.

Prerequisites: None
6 Credit Hours | 8 Week Course Term

BACS 3401: Security Essentials
SANS SEC401 | *GIAC GSEC*

BACS 3401 is a technically-oriented course in which students learn the most effective steps to prevent cyber attacks and detect adversaries. In classes and hands-on labs, students learn the essential information security skills and techniques needed to protect and secure critical information and technology assets, whether on-premise or in the cloud. Student will also learn how to directly apply the concepts learned in developing a winning defensive strategy, all in the terms of the modern adversary.

Prerequisites: BACS 3275
4 Credit Hours | 8 Week Course Term

BACS 3504: Hacker Tools, Techniques, and Incident Handling
SANS SEC504 | *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

4 Credit Hours | 8 Week Course Term

BACS 3402: Effective Cyber Writing and Speaking
SANS SEC402 & SEC403 | *No GIAC exam*

BACS 3402 strengthens students' writing and speaking skills. During the first half of the course, students 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 students the skills to put together an effective security briefing, secure the interest and engagement of their audience, and confidently deliver presentations to a variety of groups.

Prerequisites: BACS 3275
3 Credit Hours | 8 Week Course Term

BACS 3373: Introductory Python
SANS.edu online course | *pyWars Labs* | *No GIAC exam*

In this hands-on course, students actively write Python code, so can see successful results and learn by doing. Students learn how to install and maintain Python programs and modules, and utilize basic Python programming concepts such as functions, Integrated Development Environments (IDEs), modules, lists, and basic file input / output.

Prerequisites: BACS 3275
3 Credit Hours | 8 Week Course Term

BACS 3573: AI-Powered Security Automation: Building Tools with Python, LLMs and MCP
SANS SEC573 | *Additional Labs* | *GIAC GPYC*

BACS 3573 teaches students 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 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. Student learning is supported and reinforced by capture-the-flag challenges provided in the *pyWars* lab environment. Students 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, BACS 3373
4 Credit Hours | 8 Week Course Term

BACS 3001 – Portfolio Practicum: Experiential Learning Through Cyber Challenges (Foundational)
**__Note__: This course can be taken concurrently with other courses in Block 1 of the program (except BACS 3275)*

This practicum course provides hands-on experiential learning opportunities in cybersecurity through participation in national cyber challenges. Students will engage with content that will enhance technical skills, critical thinking abilities, and problem-solving techniques essential for success in cybersecurity competitions.

In this course, students will prepare for and compete in a capture-the-flag competition that will provide experience in solving real-world cybersecurity challenges. By strategically incorporating experience in a cyber challenge into their resume or portfolio, students will be better placed to effectively demonstrate skills, knowledge, and passion for cybersecurity to prospective employers.

Prerequisites: BACS 3275
3 Credit Hours | 16 Week Course Term

Block 2

BACS 3500: Windows Forensic Analysis
SANS FOR500 | *GIAC GCFE*

BACS 3500 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
4 Credit Hours | 8 Week Course Term

BACS 3503: Network Monitoring and Threat Detection In-Depth
SANS SEC503 | *Supplemental Materials* | *GIAC GCIA*
BACS 3503 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
4 Credit Hours | 8 Week Course Term

Field Experience Practicum
**Note: Practicum courses can be taken concurrently with other courses in Block 2 of the program*

Choose one of the following options:

BACS 4499: Internet Storm Center 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 16 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. See internship technology requirements in *Software and Technology Requirements.*

BACS 4001 - External Internship in Cybersecurity
BACS 4001 provides students with an opportunity to gain hands-on experience in the field of cybersecurity through an approved external internship. By working with an organization in a cybersecurity role, students will apply theoretical knowledge in real-world contexts, enhance technical skills, and build professional networks. The internship must involve a minimum of 80% cybersecurity-related tasks, with limited administrative duties, ensuring the experience aligns with the student's career aspirations and academic goals.

Students will work under the supervision of a professional mentor, set personal goals for the internship, and complete reflective and evaluative assignments to document their progress and learning. This course supports career development by helping students gain practical, industry-relevant experience while earning academic credit.

Prerequisites: BACS 3504 and BACS 3573
Recommended preparation: BACS 4503
4 Credit Hours | 16 Week Course Term

BACS 3002 – Portfolio Practicum: Experiential Learning Through Cyber Challenges (Advanced)

**Note: Practicum courses can be taken concurrently with other courses in Block 2 of the program*

This course builds on the foundational cyber challenge experience from Block 1. Students will take on more complex CTF scenarios, develop additional skills, and be encouraged to take on leadership roles in team-based challenges. Reflecting on CTF participation from *BACS 3001*, students will explore their cybersecurity strengths and weaknesses before participating in a second Capture the Flag (CTF) competition.

Students will further develop and demonstrate skills that they can showcase to prospective employers, and will use their advanced CTF experience to enhance their professional portfolio.

Prerequisites: All BACS Block 1 courses
3 Credit Hours | 16 Week Course Term

Technical Elective Course Options

ACS 4410: ICS/SCADA Security Essentials
SANS ICS410 | *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 SEC450 | *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 4456: Essentials for NERC Critical Infrastructure Protection
SANS ICS456 | *GIAC GCIP*

ACS 4456 empowers students with knowledge of the what and the how of the Critical Infrastructure Protection (CIP) Reliability Standards versions 5/6/7. The course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), and Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems, and helps asset owners determine the requirements applicable to specific implementations.

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

ACS 4497: Practical Open-Source Intelligence (OSINT)
SANS SEC497 | *GIAC GOSI*

ACS 4497 is a foundational course in open-source intelligence (OSINT) gathering that teaches students practical, real-world tools and techniques to help them perform OSINT research safely and effectively. The course not only covers critical OSINT tools and techniques, it also provides real-world examples of how they have been used to solve a problem or further an investigation. Hands-

on labs based on actual scenarios provide students with the opportunity to practice the skills they learn and understand how those skills can help in their research.

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

ACS 4498: Digital Acquisition and Rapid Triage
SANS FOR498 | *GIAC GBFA*

ACS 4498 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 4501: Advanced Enterprise Defender
SANS SEC501 | *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 4502: Cloud Security Tactical Defense
SANS SEC502 | *GIAC GCLD*

ACS 4502 equips practitioners with advanced, hands-on experience to secure modern cloud environments against evolving threats. Through live labs in real cloud environments, students will design and enforce tactical controls across identity, data, and network layers, addressing real-world risks like misconfigurations, privilege escalation, credential theft, data theft, and lateral movement. With 40 immersive, live-fire labs and a competitive Capture the Flag challenge, participants gain the expertise to harden cloud infrastructure, lead incident response efforts, and implement security strategies aligned with enterprise-scale deployments and compliance frameworks.

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

ACS 4508: Advanced Digital Forensics, Incident Response, & Threat Hunting
SANS FOR508 | *GIAC GCFA*

ACS 4508 teaches students 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: AWS, Azure, and GCP
SANS SEC510 | *GIAC GPCS*

ACS 4510 provides students 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 SEC511 | *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 4515: ICS Visibility, Detection, and Response
SANS ICS515 | *GIAC GRID*

ACS 4515 will help students gain visibility and asset identification in Industrial Control System (ICS)/Operational Technology (OT) networks, monitor for and detect cyber threats, deconstruct ICS cyber attacks to extract lessons learned, perform incident response, and take an intelligence-driven approach to executing a world-leading ICS cybersecurity program to ensure safe and reliable operations.

Prerequisites: BACS 4410
3 Credit Hours | 8 Week Course Term

ACS 4522: Defending Web Applications Security Essentials
SANS SEC522 | *GIAC GWEB*

ACS 4522 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 SEC540 | *GIAC GCSA*

ACS 4540 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 SEC542 | *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: Enterprise Penetration Testing
SANS SEC560 | *GIAC GPEN*

Both the offensive teams and defenders of an enterprise have the same goal: keep the real bad guys out. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specifically developed to get students ready for that role. ACS 4560 is designed to strengthen penetration testers and further add to their skillset. The course is also designed to train system administrators, defenders, and others in security to understand the mindset and methodology of a modern attacker. Students will learn how to plan, prepare, and execute a penetration test in a modern enterprise. Using the latest penetration testing tools, students will undertake extensive hands-on lab exercises to learn the methodology of experienced attackers and practice their skills.

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

ACS 4566: Implementing & Auditing the Critical Security Controls
SANS SEC566 | *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 students to ensure that their 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 students 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 SEC575 | *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 4577: Linux Incident Response and Threat Hunting
SANS FOR577 | *GIAC GLIR*

ACS 4577 provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including advanced persistent threat (APT) nation-state adversaries, organized crime syndicates, and hacktivism. Constantly updated, the course addresses today's incidents by teaching hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to combat real-world breach cases. The course also supports preparation for the GLIR certification (GIAC Linux Incident Response), a credential that validates your expertise in Linux threat hunting and Linux incident response within enterprise environments.

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

ACS 4588: Cloud Penetration Testing
SANS SEC588 | *GIAC GCPN*

ACS 4588 equips students with the latest in cloud-focused penetration testing techniques and teaches them 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. Students 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

ACS 4595: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals
SANS SEC595 | GIAC GMLE

ACS 4595 is squarely centered on solving information security problems. This course covers the necessary mathematics theory and fundamentals students absolutely must know to allow them to understand and apply the machine learning tools and techniques effectively. The course progressively introduces and applies various statistic, probabilistic, or mathematic tools (in their applied form), allowing students to leave with the ability to use those tools. The hands-on projects provide a broad base from which students can build their own machine learning solutions. This course teaches how AI tools like ChatGPT really work so that students can intelligently discuss their potential use by organizations and how to build effective solutions to solve real cybersecurity problems using machine learning and AI.

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

Credit Hours

A credit hour is the unit of measurement representing the amount of work typically required by an average student over a specified period in achieving intended learning outcomes. The SANS Technology Institute's Credit Hour Policy calculates credit hours based on reasonable approximations of instruction and student preparation work, in alignment with the credit hour as defined by the Maryland Higher Education Commission.

For standard courses, credit hours are calculated based on the total number of contact hours, including course content, assignments, and labs, in addition to the expected student preparation work, as outlined in the course syllabus.

For experiential, internship, and practicum courses, credit hours are reasonably approximated at 1 credit per 45 instructional hours.

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 Cybersecurity Fundamentals undergraduate certificate program must meet the following criteria:

- Have completed at least 12 college credits from a recognized college or university
- A cumulative GPA (grade point average) of 2.8 or greater

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

- Have completed at least 24 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 of the 70 required transferrable college credits from a recognized college or university, including 31 credits that meet the general education requirements
- A GPA of 3.0 or greater

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

a) Application Form
b) Current Resume
c) Official Transcripts
d) Aptitude Assessment
e) Application Fee
f) Requirements for International Students
    a. Transcript Evaluation through one of our partners
    b. Non-native English speakers must submit English proficiency scores from one of our approved assessment exams.

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 and beginning the first course within three months 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.

Registration

Students must register for courses using personalized instructions provided by their student advisor. These instructions are unique to each student and are not publicly available. Registrations paid for through SANS.org are not transferrable to SANS.edu. This policy is strictly enforced.

Course Registration Deadline

To meet course start deadlines, students must register (with tuition paid in full) at least 7 calendar days before their chosen start date. For students residing outside of the United States, it is recommended to register at least 14 days in advance. These deadlines ensure adequate processing time for tuition payments and book shipments. Late registrations will not be accepted. Students who submit registrations within the 7-day window will have their start date deferred to the next available course start date. For registration questions and/or instructions, please contact your assigned student advisor.

Course Start Dates by Modality

Courses in the OnDemand or other distance-learning modalities start on the 1st and 15th of each month unless otherwise noted. The schedule of live courses offered in the In-Person or Live-Online modalities is available at www.sans.org/cyber-security-courses. The start date for live courses is the first day of the class at the scheduled SANS training event.

Add/Drop Policy

To support student success and ensure a smooth start to the course term, enrollments must be finalized at least one week before the first day of class.

- Add/Drop Deadline: Students must add or drop a course at least 7 calendar days prior to the start date listed in their SANS.edu course syllabus.
    - Students may drop a course only if they have not accessed the online course or received the shipment of course materials.
- After this deadline, changes to enrollment, including withdrawals, modality changes, schedule adjustments, or section transfers, are not be permitted.

Tuition refunds or credits will not be issued for courses dropped on or after the first day of the course. See the "Cancellation and Change Fees" section below for associated fees.

We encourage students to carefully review their course schedules, commitments, and materials before the deadline to ensure the best fit for their academic goals. For exceptional cases (e.g., medical or family emergencies), students may submit a formal appeal with supporting documentation to the Dean of Students Office at deanofstudents@sans.edu.

Tuition and Fees

Students pay tuition on a per course basis and are responsible for tuition at the time of registration for each course. Students are expected to pass each course before starting another. Therefore, students may only register and pay for one course at a time, except when approved to overlap terms with another class. See Maximum Enrolled Credit Limits in the Student Handbook.

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. The cost of travel and lodging is in addition to the cost of tuition, for students who choose to attend in-person courses. Additional fees may also apply (e.g., application fees, exam retake fees).

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

Certificate Program in Cybersecurity Fundamentals

The table below reflects tuition rates for the Cybersecurity Fundamentals (CSF) Certificate Program.

Course	Course Cost	Credits
CSF 2395	$ 750	3
CSF 2373	$ 750	3
CSF 2275	$1,400	6
CSF Program Total	***$2,900***	***12***

Certificate Program in Applied Cybersecurity

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

Course	Course Cost	Credits
ACS 3275	$1,400	3
ACS 3401	$5,700	3
ACS 3504	$5,700	3
ACS Elective	$5,700	3
ACS Program Total	***$18,500***	***12***

Bachelor's Degree Programs in Applied Cybersecurity

The table below reflects tuition rates for the Applied Cybersecurity Bachelor's (BACS) Program.

Course	Course Cost	Credits
BACS 3275	$1,500	6
Portfolio Practicum – BACS 3001	$500	3
BACS 3401	$4,500	4
BACS 3504	$4,500	4
BACS 3402	$1,500	2
BACS 3373	$750	3
BACS 3573	$4,500	4
Field Experience Practicum – BACS 4499 / 4001	$1000	4
BACS 3500	$4,500	4
BACS 3503	$4,500	4
ACS elective	$4,500	3
ACS elective	$4,500	3
ACS elective	$4,500	3
Portfolio Practicum – BACS 3002	$500	3
BACS Program Total	***$41,750***	***50***

BACS single course discount for ACS completers

Individuals who earn the SANS.edu Applied Cybersecurity undergraduate certificate may receive one free course in the Bachelor of Applied Cybersecurity program. This course discount can only be applied to the full tuition of the final course in an eligible student's BACS program of study that includes a GIAC exam.

Eligibility guidelines:

- A student's BACS program start date must be within two years of their ACS program completion date.
- A student cannot have used a SANS-sponsored scholarship to fund their ACS program (for example, the Cyber FastTrack scholarship).
- A student must have completed all transfer credits required for the BACS program and have only a final SANS/GIAC-based course remaining to earn their bachelor's degree (usually this will be the final elective).

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 $6,500 with the exception of ACS 3275 ($1,500). For any student, there is a lifetime cap of two courses as a non-degree seeking student. In the event that a non-degree seeking student does not pass a course on the first exam attempt, they are allowed to retake the exam one time. The cost of the retake exam is an additional fee. If unsuccessful after two exam attempts, the student is no longer eligible to pursue a second single course and is required to wait one year before applying to a SANS.edu program.

Fees

The following fees may apply:

Application Fee*	Varies by program
GIAC Exam Retake Fee	Set by GIAC

* Paid during the application process. Application fee amount is available on the Undergraduate Admission webpage: https://www.sans.edu/admissions/undergraduate/

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. Any arrangements and associated lodging costs 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 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.

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.

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.

SANS.edu Step Up Payment Plan (SUPP)

The SANS Technology Step Up Payment Plan (SUPP) is a monthly payment program designed to allow undergraduate students to make monthly installments towards courses taken as part of an academic program.

Step Up Payment Plan Basics

Participation Eligibility
Participants must meet these criteria:

- Be enrolled in an academic program at SANS Technology Institute
- Be a U.S. citizen
- Meet financial eligibility requirements
- Agree to utilize a U.S. bank with automated, monthly EFT payment withdrawals
- Agree to respond to communications from the Bursar's Office by phone and email

Application

- If accepted into the Step Up Payment Plan, applicants will need to provide bank details to set up automated monthly EFT withdrawals.
- Applications that are not complete within 30 days will be automatically closed.
- Due to the sensitive nature of application materials, SANS Technology Institute will securely store and transmit applicant information. Once a participant's Step Up Payment Plan account balance has been paid in full, application materials will be removed from our systems.

Monthly Payments

- On the 1st day of each month, all current Step Up Payment Plan users will be scheduled for a payment to be withdrawn on the 15th. Any requested changes to a Step Up Payment Plan participant's bank account needs to be communicated to the Bursar's Office prior to the 1st of the month.
- As is customary for intra-bank transfers, the transactions will be initiated a few days prior to the 15th of the month, so participants shall ensure adequate funds are available in their account by the 10th of the month to avoid insufficient funds.
- Monthly payment amounts will be directly withdrawn on the 15th of the month. If the 15th of the month falls on a weekend or bank holiday, the payment may be delayed a few days.
- Once the monthly payments have cleared, an email receipt will be sent to participants.
- Payments that are rejected due to insufficient funds are subject to the Late Payment policy below.
- Monthly payments will not be paused between courses, or while a student is on a Leave of Absence and a balance remains on their Step Up Payment Plan Account.
- Step Up Payment Plan participants will pay $350 per month for each month they are currently enrolled in their academic program or on a Leave of Absence. Once the student exits their academic program (either through program completion, withdrawal, or dismissal), their payment will be $650 per month until the account balance is paid off.

Step Up Payment Plan Policies

Account Balance

- Approved applicants will be permitted to register for courses up to the maximum tuition amount needed to complete their academic program. This amount is subject to change based upon waived courses, tuition increases, or retaking failed courses. Retake exams are paid directly to GIAC and cannot be added to a Step Up Payment Plan account balance.
- Approved participants will be provided with a code to be used at the time of course registration. By using this code, the tuition associated with that course will be added to their Step Up Payment Plan account balance. Participants shall not share their Step Up Payment Plan code with any other students.
- Participants are financially responsible for paying the total tuition amount for all courses in which a participant has registered using their Step Up Payment Plan code and started the course, regardless of their participation or course grade.
- Participants who wish to use alternative funds such as employer tuition assistance or VA Education Benefits to pay for a course may do so. However, multiple payment methods cannot be combined in a single course registration. By using an alternative funding method, the associated tuition will be removed from the Step Up Payment Plan account balance.
- Monthly payments are applied towards a participant's Step Up Payment Plan account balance, and not towards a specific course registration. As a result, students will not receive a "Paid" invoice for individual courses when utilizing the Step Up Payment Plan; these invoices show as "Comped".
- A detailed Step Up Payment Plan account ledger can be requested by emailing bursar@sans.edu.

Late Payments

- Monthly payments that are rejected due to insufficient funds will be considered "Late" and incur a $25 fee. The SANS.edu Bursar will notify participants by email and provide instructions to call in a credit card payment. Participants are expected to submit their late payment and fee within 5 days of being notified.
- If late payments are not resolved within 10 days of the original payment date, the participant will be dismissed from the Step Up Payment Plan Program and be subject to the policies for Closing a Step Up Payment Plan Account below.
- If late payments are not resolved within 30 days of the original payment date, the participant may be dismissed from their academic program, with a hold on their official academic records.
- Participants are permitted a total of 2 late payments over the duration of their participation in the Step Up Payment Plan. Upon a third late payment, participants will be dismissed from the Step Up Payment Plan and be subject to the policies for Closing a Step Up Payment Plan Account below.

Additional Payments

- Participants can submit additional lump sum payments to reduce the number of monthly payments on the back end of the payment terms. Additional payments will not substitute for regular monthly payments.
- Additional payments can be submitted in two ways:
    - Calling in a credit card payment
    - Increasing the amount of the next month's payment
- Students wishing to submit an additional payment should email bursar@sans.edu for further instructions.

Closing a Step Up Payment Plan Account

- Participants can withdraw from the Step Up Payment Plan at any time without penalty.
- Participants who withdraw, or are dismissed, from the Step Up Payment Plan are responsible for paying off their remaining Step Up Payment Plan account balance before registering for any additional courses through SANS.edu. Participants are not responsible for the tuition of any course that was not registered for and started.
- Participants who withdraw, or are dismissed, from the Step Up Payment Plan and have a credit on their Step Up Payment Plan account will be issued a refund via check.
- Participants who are dismissed from their academic program will continue to make monthly payments until their Step Up Payment Plan account balance is paid off.
- Participants who do not resolve late payments as directed may be dismissed from SANS Technology Institute with a hold on their academic records.
- Tuition balances not paid by the due date may be sent to collections and incur additional fees of up to 35% of the balance due. In addition, participants will be responsible for all fees and costs incurred by SANS in collecting the debt owed, including collection costs, attorneys' fees, and judicial expenses.
- If participants file for bankruptcy while participating in the Step Up Payment Plan, they are still required to pay off any remaining Step Up Payment Plan account balance.
- SANS Technology Institute reserves the right to dismiss Step Up Payment Plan participants at any time if we have reason to believe a participant committed fraud in connection with the Step Up Payment Plan application.

Miscellaneous

- SANS Technology Institute reserves the right to modify the policies and procedures associated with the Step Up Payment Plan. The current Step Up Payment Plan policies will be published in the Course Catalog and can be accessed on our website. By remaining in the Step Up Payment Plan, participants are agreeing to abide by these policies.

SANS.edu Tuition Payment Program (TPP)

The SANS Technology Institute Tuition Payment Program (TPP) is a monthly payment program designed to allow undergraduate students without alternative funding options to make monthly installments towards courses taken as part of an academic program. The TPP is not a student loan and does not incur interest.

TPP Basics

Participation Eligibility

To be eligible for the SANS Technology Institute Tuition Payment Program (TPP), participants must meet these criteria:

- Be enrolled in an upper division undergraduate certificate program or the bachelor's program at SANS Technology Institute
- Be a U.S. citizen
- Meet financial eligibility requirements
- Agree to utilize a U.S. bank with automated, monthly EFT payment withdrawals
- Agree to respond to communications from the Bursar's Office by phone and email

Application

- Participants can apply before or during their academic program at SANS.edu through our application portal.
- Applicants are required to provide financial information including: monthly income, monthly expenses, proof of income, Experian credit report, and other financial documents requested by the TPP Committee.
- If accepted into the Tuition Payment Program, applicants will need to provide bank details to set up automated monthly EFT withdrawals.
- Applications that are not complete within 30 days will be automatically closed.
- Due to the sensitive nature of application materials, SANS Technology Institute will securely store and transmit applicant information. Once a participant's TPP account balance has been paid in full, application materials will be removed from our systems.

Monthly Payments

- On the 1st day of each month, all current TPP users, including recently admitted students, will be scheduled for a payment to be withdrawn on the 15th. Any requested changes to a TPP participant's bank account needs to be communicated to the Bursar's Office prior to the 1st of the month.

- As is customary for intra-bank transfers, the transactions will be initiated a few days prior to the 15th of the month, so participants shall ensure adequate funds are available in their account by the 10th of the month to avoid insufficient funds.
- Monthly payment amounts will be directly withdrawn on the 15th of the month. If the 15th of the month falls on a weekend or bank holiday, the payment may be delayed a few days.
- Once the monthly payments have cleared, an email receipt will be sent to participants.
- Payments that are rejected due to insufficient funds are subject to the Late Payment policy below.
- Monthly payments will not be paused between courses, or while a student is on a Leave of Absence and a balance remains on their TPP Account.

TPP Policies

TPP Account Balance

- Approved applicants will be permitted to register for courses up to the maximum tuition amount needed to complete their academic program. This amount is subject to change based upon waived courses, tuition increases, or retaking failed courses. Retake exams are paid directly to GIAC and cannot be added to a TPP account balance.
- Approved TPP participants will be provided with a code to be used at the time of course registration. By using this code, the tuition associated with that course will be added to their TPP account balance. Participants shall not share their TPP code with any other students.
- Participants are financially responsible for paying the total tuition amount for all courses in which a participant has registered using their TPP code and started the course, regardless of their participation or course grade.
- Participants who wish to use alternative funds such as employer tuition assistance or VA Education Benefits to pay for a course may do so on a limited basis. However, multiple payment methods cannot be combined in a single course registration. By using an alternative funding method, the associated tuition will be removed from the TPP account balance.
- Monthly payments are applied towards a participant's TPP account balance, and not towards a specific course registration. As a result, students will not receive a "Paid" invoice for individual courses when utilizing the TPP; these invoices show as "Comped".
- A detailed TPP account ledger can be requested by emailing bursar@sans.edu.
- Participants can only have one active TPP account at a time. If a participant begins another program and would like to use TPP, there are two options:
    - Make a one-time payment to pay the remaining balance in full, or
    - Continue with the monthly auto-draft payments until the balance is fully paid. Once the balance is cleared, students can contact the Bursar's office to proceed with using TPP for a second program. If you choose to continue with the auto-draft payments, you may still move forward with a new program, but will need to provide an alternative payment method, as TPP cannot be used until the balance from a prior program has been paid in full.

Late Payments

- Monthly payments that are rejected due to insufficient funds will be considered "Late" and incur a $25 fee. The SANS.edu Bursar will notify participants by email and provide

instructions to call in a credit card payment. Participants are expected to submit their late payment and fee within 5 days of being notified.
- If late payments are not resolved within 10 days of the original payment date, the participant will be dismissed from the Tuition Payment Program and be subject to the policies for Closing a TPP Account below.
- If late payments are not resolved within 30 days of the original payment date, the participant may be dismissed from their academic program, with a hold on their official academic records.
- Participants are permitted a total of 2 late payments over the duration of their participation in the TPP. Upon a third late payment, participants will be dismissed from the TPP and be subject to the policies for Closing a TPP Account below.

Additional Payments

- Participants can submit additional lump sum payments to reduce monthly payments on the back end of the payment terms. Additional payments will not substitute for regular monthly payments.
- Additional payments can be submitted in two ways:
    - Calling in a credit card payment
    - Increasing the amount of the next month's payment
- Students wishing to submit an additional payment should email bursar@sans.edu for further instructions.

Closing a TPP Account

- Participants can withdraw from the TPP at any time without penalty.
- Participants who withdraw, or are dismissed, from the TPP are responsible for paying off their remaining TPP account balance before registering for any additional courses through SANS.edu. Participants are not responsible for the tuition of any course that was not registered for and started.
- Participants who withdraw, or are dismissed, from the TPP and have a credit on their TPP account will be issued a refund via check.
- Participants who are dismissed from their academic program will continue to make monthly payments until their TPP account balance is paid off.
- Participants who do not resolve late payments as directed may be dismissed from SANS Technology Institute with a hold on their academic records.
- Tuition balances not paid by the due date may be sent to collections and incur additional fees of up to 35% of the balance due. In addition, participants will be responsible for all fees and costs incurred by SANS in collecting the debt owed, including collection costs, attorneys' fees, and judicial expenses.
- If participants file for bankruptcy while participating in the TPP, they are still required to pay off any remaining TPP account balance.
- SANS Technology Institute reserves the right to dismiss TPP participants at any time if we have reason to believe a participant committed fraud in connection with the TPP application.

Miscellaneous

- SANS Technology Institute reserves the right to modify the policies and procedures associated with the Tuition Payment Program. The current TPP policies will be published in

the Course Catalog and can be accessed on our website. By remaining in the Tuition Payment Program, participants are agreeing to abide by these policies.

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.

Credit Transfers and Waivers

Credit Transfers

The SANS Technology Institute (SANS.edu) accepts transfer credit, waiver credit and earned credit within the guidelines described below.

Undergraduate Programs Transfer Credit

The SANS Technology Institute only accepts transfer credits completed at other schools for our bachelor's degree program. These transfer credits are required to be admitted to and graduate from the bachelor's program at SANS.edu. The degree requirements are outlined on the undergraduate admissions page.

- SANS.edu can accept a maximum of 70 college credits as transfer credit to count toward the bachelor's program.
- Accepted transfer credits receive no credit hours or grades awarded.
- All transfer credits are evaluated as part of the admissions process when applying. We do not complete unofficial evaluations based on unofficial transcripts or preliminary evaluations conducted before a student applies.
- Transfer credits are only accepted from accredited colleges and universities.
    - If the transfer credits were earned outside the U.S., they must be sent for course-by-course evaluation by one of our approved partners, found here.
- SANS.edu can only accept CLEP, AP, IB or similar test-related credits after they have been accepted by *another* college and send to us on that college's official transcript.

To be admitted to SANS.edu undergraduate certificate programs, students are required to have completed previous college work. However, the undergraduate certificate programs do not require or accept transfer credit in place of the required SANS.edu curriculum.

Transcript Appeal: If a student wants to submit an appeal related to a transfer evaluation, they can do so here: https://application.sans.edu/register/transcriptappeal. An appeal is only eligible if there is new information to submit and provide a reason for the appeal to the Transcript Committee.

Waiver Credit

"Waiver credit" refers to credit earned from previously completed SANS courses, GIAC exams, PMP or CISSP.

Waivers may be granted for up to, but not more than, one-quarter of the total number of credit hours required by a program (the "25% limit"), and are subject to the requirements as described below:

- All waivers are granted *only* prior to a student's matriculation. Students may *not* take courses outside SANS.edu for credit in their program after they matriculate.
- Course waivers receive no grades awarded. Waivers are not figured into the calculation of a student's cumulative grade point average (GPA).
- All certifications must be active and current to eligible for credit. See the GIAC renewal policies.
- **Waiver exceptions for government and military employees:** Learn about exceptions to the waiver limit, that applies to only the bachelor's degree program, in the section on Participants in Government or Military Education and Training Programshttps://www.sans.edu/admissions/transfer-of-credit/?msc=main-nav.

CISSP Certification

For students who hold a current CISSP certification from the (ISC)² organization, a waiver will be granted within ACS 3401 and BACS 3401 for the SANS class SEC401. 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 SEC401 class. Waiver eligibility will be confirmed with students' academic advisor at the time they are ready in their program for ACS/BACS 3401. *NOTE: Students who have only achieved Associate of (ISC)² status are not eligible for this waiver.*

Technology and Software Requirements

In order to fulfill the requirements of the SANS Technology Institute curriculum, students 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 classes will require special software to be loaded on students' computer. Approximately a week before class, students will receive notice of the class software requirements. This will tell students where to get any software needed for the class and labs, as well as any configuration settings that need to be applied.

Suggested Laptop Requirements

A properly configured system is required to fully participate in your courses at SANS Technology Institute (SANS.edu). Although SANS.edu does not have standardized laptop requirements applicable to all courses, below is a suggestion of requirements based on one of our more requirement-demanding courses. ***Please note that these requirements are subject to change.*** You may want to browse the laptop requirements for some of the classes you intend to take. Make sure your computer can run VMWare. As a test, download the free VMWare Player (or a trial version of VMWare Workstation) and install a Windows 10 and an Ubuntu virtual machine. Make sure they both run sufficiently well and can communicate with each other.

A modern, well configured, laptop is critical for your success in any SANS class. Exercises make up a crucial part of your learning experience. You need full administrative access to your laptop and you need to be able to configure all system settings, including BIOS. It may be necessary to disable some security features like VPNs or anti-malware products.

Laptop Requirements

- CPU: a recent 64-bit Intel/AMD (x86-64 Bit) processor. For example, Intel i5/i7 4th generation or later.
- **CRITICAL NOTE: Apple systems using the M1/M2 processor line cannot perform the necessary virtualization functionality and, therefore, cannot in any way be used for most classes. The same is true for other ARM architecture-based systems.**
- It is critical that your CPU and operating system support 64-bit so that our 64-bit guest virtual machine will run on your laptop. VMware provides a free tool for Windows that will detect whether or not your host supports 64-bit guest virtual machines. For further troubleshooting, this article also provides good instructions for Windows users to determine more about the CPU and OS capabilities. For Macs, please use this support page from Apple to determine 64-bit capability.

- BIOS settings must be set to enable virtualization technology, such as "Intel-VT". **Be absolutely certain you can access your BIOS if it is password protected**, in case changes are necessary. Test it!
- A minimum of 16GBytes of RAM is required. Many classes recommend 32GBytes.
- USB 3.0 Type-A port is required. At least one open and working USB 3.0 Type-A port is required. (A Type-C to Type-A adapter may be necessary for newer laptops.) (Note: Some endpoint protection software prevents the use of USB devices - test your system with a USB drive before class to ensure you can load the course data.)
- 1TB of SSD hard drive space. Classes may require up to 350 Gigabytes of Free Space.
- Local Administrator Access is required. This is absolutely required. Don't let your IT team tell you otherwise. If your company will not permit this access for the duration of the course, then you should make arrangements to bring a different laptop.
- **Wireless 802.11 Capability is required.**

Operating System

- Host Operating System: Latest version of Windows 10 or macOS 10.15.x
- Please note: It is necessary to fully update your host operating system prior to the class to ensure you have the right drivers and patches installed to utilize the latest USB 3.0 devices.

Technology Requirements for the ISC Internship (BACS 4499)

To participate in BACS 4499: ISC Internship, students are required to have the equipment and internet access necessary to set up a DShield honeypot. You should plan to have this equipment by the first week of the internship. There is no need to purchase this equipment if you already have it and are able to dedicate its use for the duration of the internship.

DShield Honeypot Basics

The DShield honeypot is a low interaction honeypot that allows Internet Storm Center handlers to collect data for research purposes. The honeypot by default runs the following clients:

- Collecting SSH and Telnet usernames and passwords via Cowrie
- An HTTP honeypot collecting full http requests
- Collecting firewall logs from the honeypot

The honeypot can be installed on a Raspberry Pi using Raspbian OS or a system running Ubuntu 20.04 LTS.

For more detailed information about DShield honeypot equipment and set up, review the DShield Honeypot page: https://isc.sans.edu/tools/honeypot/.

Veterans Benefits

Introduction

This section provides explanations for how 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 students receive throughout the course of their 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 students 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 students 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 that students receive are determined by the courses they might be taking at the time.

Approved Live Learning Events for 2026

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 2026:

Baltimore:

Hyatt Regency Baltimore
300 Light Street
Baltimore, MD 21201

Hilton Baltimore Inner Harbor
401 W Pratt Street
Baltimore, MD 21201

Kimpton Hotel Monaco Baltimore Inner Harbor
2 North Charles St
Baltimore, MD 21201

The Royal Sonesta Harbor Court Baltimore
550 Light Street
Baltimore, MD 21202

Columbia:

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

Rockville:

Hilton Washington DC/Rockville
1750 Rockville Pike
Rockville, MD 20852

Bethesda:

Hyatt Regency Bethesda
One Bethesda Metro Center
7400 Wisconsin Ave
Bethesda, MD 20814

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/

Costs Covered

- The VA pays the school tuition and fees directly, based on the student's eligibility percentage.

    - Example, Student A has 100% eligibility for Chapter 33 benefits, and Student B has 80% eligibility.
    - Student A would have 100% of tuition and fees covered, whereas Student B would have 80% of tuition and fees covered.
- Students needing to purchase exam retakes from GIAC **may** have the cost of the exam reimbursed by the VA.

Rate of Pursuit

As detailed earlier in the catalog, each course is itself the enrollment term as far as how we certify enrollment to the VA. This means that when we certify enrollment 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.
- The VA considers **ACS accelerated terms to be greater than half-time** enrollment when calculating one's rate of pursuit.
- The VA considers **ACS standard terms to be less than half-time enrollment** when calculating one's rate of pursuit.
- Students may complete coursework earlier than the targeted timeframe, but we will not adjust the certification as the course term remains the same.

Housing Allowance

The VA will calculate a prorated Monthly Housing Allowance 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.

The 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 (as described in the previous section), and
c. The student is not on active duty.

The calculation of MHA is impacted by the following considerations:

- 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

Please note that students should not expect MHA for exam retake attempts.

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 a student's qualification percentage. The annual cap re-sets the 1st of August each year.

Vocational Rehabilitation & Employment

Costs Covered

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.

Students will work closely with their assigned student advisors, as well as their Ch 31 counselors, as they progress through their program and maintain Ch 31 approvals.

Students needing to purchase exam retakes through GIAC should work with their assigned student advisor to ensure VA counselor approval. Please note that students should not expect subsistence allowance for exam retake attempts.

Other GI Bill® Chapters, including Chapter 30 Montgomery Bill

Costs Covered

Veterans using other GI Bill® Chapters (30, 35, 1606) receive monthly stipend payments directly from the VA, based on their enrollment term training time (full-time, ¾ time, etc.), and then they are responsible for paying tuition and fees to the College.

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.

The VA determines the amount the VA will pay students for their enrollment term, based upon calculating a veteran's training time, and **students should be advised that after their VA payments, they may still owe tuition**, the amount of which depends on their enrollment terms.

Please note:

- 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.

- The VA considers **ACS accelerated terms to be less than full-time and greater than half-time** enrollment when calculating one's training time for the 8-week term.
- The VA considers **ACS standard terms to be less than half-time enrollment** when calculating one's training time for the 13-week term.
- Students may complete coursework earlier than the targeted timeframe, but we will not adjust the certification as the course term remains the same.
- Students are encouraged to review payment rates based on training time here.

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®" as payment method. This provides SANS.edu with consent to be "certified" with the VA for the course.
2) The College will certify enrollment to the VA, regardless of benefits chapter, to trigger the tuition payment process.
3) 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.

Tuition & Fees

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
- Students using Chapter 30 or Chapter 1606 benefits (as they will receive less than total tuition cost for ACS courses)
- Student stops meeting attendance requirements in a course that was certified to the VA
- Student's benefit expires during enrollment term (the "delimiting date" on the Certificate of Eligibility)

Tuition balances not paid by the due date may be sent to collections and incur additional fees up to 35% of the balance due. In addition, you will be responsible for all fees and costs incurred by SANS in collecting the debt owed, including collection costs, attorneys' fees, and judicial expenses.

Please note:

- Students using GI Bill® benefits will not be penalized while the College awaits payment from the Department of Veteran Affairs.
- Students 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 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 generate a tuition debt with the College as well as to the VA for any associated MHA.
- Students who fail their exam attempt need not worry about generating any VA debt due to their exam failure.
- Verify enrollment
    - Students using Ch 30 benefits must verify their enrollment to receive payments from the VA; review guidance here.
    - Students using Ch 33 benefits must verify their enrollment to receive MHA payments from the VA; review guidance here.
- Report address changes
    - Students using VR&E who move may be reassigned to a new VR&E counselor. Students must inform this change to veterans@sans.edu.

Students using other GI Bill® chapters must keep their mailing address updated to ensure timely delivery of benefits related information.

Course Attendance Requirements

- Students using GI Bill® must adhere to the course benchmarks outlined in the syllabus to demonstrate course attendance for GI Bill®, regardless of the modality in which the course is taken.
- If a student using GI Bill® stops attending and does not complete a course, we are required to inform the VA of their last date of participation. The VA defines this situation as having unofficially withdrawn from the course and schools must report enrollment changes.
- This enrollment change will result in the student ultimately bearing responsibility for any tuition and MHA issued. The VA will seek a tuition from the school, and the student will then owe the school that tuition debt, due within 60 days of debt notification.

- If a student using GI Bill® requests and is awarded an incomplete grade, their VA certification for the course term will not be amended and therefore, no additional benefits will be received. Students who owe a tuition balance are not eligible for an incomplete grade.
- Students are expected to maintain satisfactory academic progress as outlined in the *Student Handbook*.

VA Requirements of SANS Technology Institute

Monitor Course and Program Progress

SANS.edu will monitor students' course attendance to ensure that they are progressing appropriately. We track course attendance by checking how successfully students have met course milestone due dates. Additionally, students are 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) ~7 days prior to the first day of the term, regardless of modality.

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 student enrollment status to the VA. Enrollment changes could include withdrawals (official or unofficial), change course date, change delivery modality, etc. These changes could affect a student's rate of pursuit which could impact their stipend and/or benefits payments. We also report academic progress (including 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 a student's records for a minimum of 3 years following the termination of their enrollment.

What students can expect from the VA

Benefit Letters

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

Payments

- Chapter 30: The VA will deposit money directly into the bank account students have provided to them.
- Chapter 33, Chapter 31: The VA will send funds for tuition and fees directly to SANS Technology Institute and deposit funds for the book stipend and MHA to the student.

VA Resources and Contact Information

While we will make every effort to help students navigate their benefits, it is ultimately the student's responsibility to understand their 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 students find the information they 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, 1747 North Market Blvd., Suite 225, Sacramento, California, 95834, (916) 574-8900 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 noncollection 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.

Course Catalog Archive

The current version of this Course Catalog can be accessed via the SANS Technology Institute's Student Consumer Information web page:
https://www.sans.edu/about/student-consumer-information/

Archived versions of SANS Technology Institute's Course Catalogs and other academic documents can be accessed using the following website:

https://web.archive.org/

To access a previous version of this document, enter the URL of the current version of the document shown on the Student Consumer Information page into the search bar. From there, you can search by date to find the document version that you require.