**(Prerequisite: CIS 175 or CIS 170 for Criminal Justice majors only)**

**COURSE DESCRIPTION**

This is a lab-based course that provides an overview of information technology security principles, challenges, vulnerabilities and countermeasure strategies. Topics include definition of security terms, concepts, elements, and goals. Students will explore industry standards and practices that focus on the availability, integrity and confidentiality aspects of information systems security.

**ADDITIONAL COURSE OBJECTIVE**

In addition to academic credit, this course is designed to prepare students to take the CompTIA Security+ certification exam and the TestOut Security Pro certification exam. The specific criteria to take these exams may include prerequisite exams or time in the profession. Students intending to take the CompTIA Security+ examination should review the published requirements by CompTIA to verify that they meet the qualifications. Preparing to pass the CompTIA Security+ certification exam may also require exam self-study that does not count toward students’ course grade. Successfully completing this course does not guarantee a student will pass the certification exam.

**INSTRUCTIONAL MATERIALS**

**Required Resources**

TestOut Security Pro (2015). ISBN: 978-1-935080-44-2

**Note:** TestOut Security Pro has built in labs. It is a code and must be purchased by all students from the Strayer Bookstore: <http://www.strayerbookstore.com/>. There is no way to complete this class without access to TestOut labs. Review the Week 1 Notes section of the Course Guide for information regarding TestOut LabSim access and registration information.

**Supplemental Resources**

CompTIA. (2017). Retrieved from <https://www.comptia.org/>

National Security Agency (NSA). (2014). Retrieved from <http://www.nsa.gov>

Network World. (2014). Retrieved from <https://www.networkworld.com/topics/security.html>

**COURSE LEARNING OUTCOMES**

1. Explain the concepts of information systems security.
2. Describe the principles of risk management.
3. Assess the means attackers use to compromise IT systems.
4. Describe the ethical principles in information security.
5. Analyze the importance of network architecture to security operations.
6. Apply information security standards to real-world implementation.
7. Communicate how problem-solving concepts are applied in a business environment.
8. Use information resources to research issues in information systems security.
9. Write clearly about network security topics using proper writing mechanics and business formats.

**TESTOUT**

This course guide outlines the due dates for your weekly work in TestOut, including labs, videos, other learning materials, and assessments. These due dates are governed by the late policy for the school. Please note that your most recent score will be recorded in the official gradebook here in Blackboard (Bb). STUDENTS ARE REQUIRED to keep a close eye on their grades transferring over from TestOut to ensure accuracy. Students are encouraged to work through all weekly TestOut labs and materials thoroughly and to re-take the weekly TestOut assessments as many times as they’d like PRIOR to the due date. If you wish to request to complete a TestOut assessment after the due date has passed, you must reach out to your instructor. Instructors have discretion on how flexible to be regarding the late policy. The final TestOut Security Pro certification exam in Week 11 may only be taken once.

**WEEKLY COURSE SCHEDULE**

The standard requirement for a 4.5 credit hour course is for students to spend 13.5 hours in weekly work. This includes preparation, activities, and evaluation (regardless of delivery mode).

Aside from a written assignment and weekly discussion questions, all the learning activities in this course take place in TestOut. Here, you’ll work through videos, demonstrations, fact sheets, practice questions, and — most importantly — lab simulations and weekly assessments to prepare for the CompTIA Security+ certification exam. You can retake the weekly assessments (Weeks 1-10) as many times as you want until the due date to improve your grade. At the due date, the most recent score will be kept.

It’s important to monitor your progress and use the TestOut reports to keep on target.

| **Week** | **Learning Activities and Evaluation** | **Points** |
| --- | --- | --- |
| 1 | **Security Overview, Access Control, and Identity Management**  TestOut Security Pro:   * + <http://www.strayer.edu/cert-prep-exam-vouchers>   *ACTIVITIES*   * Introductions: Please introduce yourself to your peers and your professor. Discuss your career goals. * TestOut Security Pro   + Chapter 1: Introduction     - Section 1.1: Security Overview     - Section 1.2: Using the Simulator   + Chapter 2: Access Control and Identity Management     - Section 2.1: Understanding Attacks     - Section 2.2: Defense Planning     - Section 2.3: Access Control     - Section 2.4: Cryptography Basics     - Section 2.5: Network Monitoring     - Section 2.6: Incident Response   *EVALUATION*   * Week 1 TestOut Assessment Note: The weekly assessments have unlimited attempts until the due date.   *DISCUSS*   * Discussion Question: Your Learning Progress   This week, you’ve covered a lot of ground in your TestOut labs. The goal of the discussion is to get students involved with each other in the learning process. Your instructor may be an expert, but you’re rapidly becoming one!  Sharing what you learn is an important part of learning. It will help you solidify the things you’ve learned and will help others see things from your perspective.   * + By Wednesday, post your thoughts on the top three things you learned.   + On Thursday or Friday, read some postings made by classmates and comment on some (at least two) that interest you.   + On Saturday or Sunday, return and post your replies to the conversation that’s going on. If no one has replied to you, find some other posts you find interesting and join the conversation.   Remember to give substantive explanations of your items. Use professional language and not text speak, just like you will/do in the business world. Don’t forget to have fun!   * Optional Discussion: Comprehensive Certification Readiness (optional and not graded but recommended) located in the Blackboard course shell. | 60  10 |
| 2 | **Policies, Procedures, and Awareness**  *ACTIVITIES*   * TestOut Security Pro   + Chapter 3: Policies, Procedures, and Awareness * Section 3.1: Security Policies * Section 3.2: Risk Management * Section 3.3: Business Continuity * Section 3.4: Manageable Network Plan * Section 3.5: Social Engineering * Section 3.6: App Development and Deployment * Section 3.7: Employee Management * Section 3.8: Mobile Devices * Section 3.9: Third-Party Integration   + Physical * Section 4.1: Physical Threats   *EVALUATION*   * Week 2 TestOut Assessment   *DISCUSS*   * Discussion Question: Your Learning Progress   Post the top three things you learned this week, read and comment to your peers, and then post one item you’d like to learn.   * Optional Discussion: Comprehensive Certification Readiness (optional and not graded but recommended) located in the Blackboard course shell. | 60  10 |
| 3 | **Physical Security**  *ACTIVITIES*   * TestOut Security Pro   + Chapter 4: Physical (Continued) * Section 4.2: Device Protection * Section 4.3: Network Infrastructure Protection * Section 4.4: Environmental Controls   + Chapter 5: Perimeter * Section 5.1: Recon and Denial * Section 5.2: Spoofing and Poisoning * Section 5.3: Security Appliances * Section 5.4: Demilitarized Zones (DMZ) * Section 5.5: Firewalls * Section 5.6: Network Address Translation (NAT) * Section 5.7: Virtual Private Networks (VPN)   *EVALUATION*   * Week 3 TestOut Assessment   *DISCUSS*   * Discussion Question: Your Learning Progress   Post the top three things you learned this week, read and comment to your peers, and then post one item you’d like to learn.   * Optional Discussion: Comprehensive Certification Readiness (optional and not graded but recommended) located in the Blackboard course shell. | 60  10 |
| 4 | **Physical Security and Network**  *ACTIVITIES*   * TestOut Security Pro   + Chapter 5 (Continued): Perimeter * Section 5.8: Web Threat Protection * Section 5.9: Network Access Protection * Section 5.10: Wireless Overview * Section 5.11: Wireless Attacks * Section 5.12: Wireless Defenses   + Chapter 6: Network * Section 6.1: Network Threats * Section 6.2: Network Device Vulnerabilities * Section 6.3: Network Applications * Section 6.4: Switch Attacks * Section 6.5: Switch Security   *EVALUATION*   * Week 4 TestOut Assessment   *DISCUSS*   * Discussion Question: Your Learning Progress   Post the top three things you learned this week, read and comment to your peers, and then post one item you’d like to learn.   * Optional Discussion: Comprehensive Certification Readiness (optional and not graded but recommended) located in the Blackboard course shell.   *EVALUATION*   * First draft of Assignment 1: Creating and Communicating a Security Strategy is due. | 60  10 |
| 5 | **Network Security**  *ACTIVITIES*   * TestOut Security Pro   + Chapter 6 (Continued): Network * Section 6.6: Using VLANs * Section 6.7: Router Security * Section 6.8: Intrusion Detection and Prevention * Section 6.9: Vulnerability Assessment * Section 6.10: Protocol Analyzers * Section 6.11: Remote Access * Section 6.12: Network Authentication * Section 6.13: Penetration Testing * Section 6.14: Virtual Networking   *EVALUATION*   * Week 5 TestOut Assessment   *DISCUSS*   * Discussion Question: Your Learning Progress   Post the top three things you learned this week, read and comment to your peers, and then post one item you’d like to learn.   * Optional Discussion: Comprehensive Certification Readiness (optional and not graded but recommended) located in the Blackboard course shell. | 60  10 |
| 6 | **Network and Host Defenses**  *ACTIVITIES*   * TestOut Security Pro   + Chapter 6 (Continued): Network * Section 6.15: Software-Defined Networking (SDN) * Section 6.16: Cloud Services   + Chapter 7: Host Defenses * Section 7.1: Malware * Section 7.2: Password Attacks * Section 7.3: Windows System Hardening * Section 7.4: Hardening Enforcement * Section 7.5: File Server Security * Section 7.6: Linux Host Security * Section 7.7: Embedded Systems * Section 7.8: Log Management * Section 7.9: Audits   *EVALUATION*   * Week 6 TestOut Assessment * Assignment 1: Creating and Communicating a Security Strategy is due.   *DISCUSS*   * Discussion Question: Your Learning Progress   Post the top three things you learned this week, read and comment to your peers, and then post one item you’d like to learn.   * Optional Discussion: Comprehensive Certification Readiness (optional and not graded but recommended) located in the Blackboard course shell. | 60  100    10 |
| 7 | **Host Defenses and Application Security**  *ACTIVITIES*   * TestOut Security Pro   + Chapter 7 (Continued): Host Defenses * Section 7.10: Email * Section 7.11: BYOD Security * Section 7.12: Mobile Device Management * Section 7.13: Host Virtualization   + Chapter 8: Application * Section 8.1: Access Control Models * Section 8.2: Authentication * Section 8.3: Authorization * Section 8.4: Web Application Attacks * Section 8.5: Internet Browsers   *EVALUATION*   * Week 7 TestOut Assessment   *DISCUSS*   * Discussion Question: Your Learning Progress   Post the top three things you learned this week, read and comment to your peers, and then post one item you’d like to learn.   * Optional Discussion: Comprehensive Certification Readiness (optional and not graded, but recommended) located in the Blackboard course shell. | 60  10 |
| 8 | **Application Security**  *ACTIVITIES*   * TestOut Security Pro   + Chapter 8 (Continued): Application * Section 8.6: Application Development * Section 8.7: Active Directory Overview * Section 8.8: Windows Domain Users and Groups * Section 8.9: Linux Users * Section 8.10: Linux Groups * Section 8.11: Linux User Security * Section 8.12: Group Policy Overview   *EVALUATION*   * Week 8 TestOut Assessment   *DISCUSS*   * Discussion Question: Your Learning Progress   Post the top three things you learned this week, read and comment to your peers, and then post one item you’d like to learn.   * Optional Discussion: Comprehensive Certification Readiness (optional and not graded but recommended) located in the Blackboard course shell. | 60  10 |
| 9 | **Application and Data Defenses**  *ACTIVITIES*   * TestOut Security Pro   + Chapter 8 (Continued): Application * Section 8.13: Hardening Authentication 1 * Section 8.14: Hardening Authentication 2   + Chapter 9: Data * Section 9.1: Data Management * Section 9.2: Advanced Cryptography * Section 9.3: Cryptography Implementations * Section 9.4: Cryptographic Attacks * Section 9.5: Symmetric Encryption * Section 9.6: Asymmetric Encryption   *EVALUATION*   * Week 9 TestOut Assessment   *DISCUSS*   * Discussion Question: Your Learning Progress   Post the top three things you learned this week, read and comment to your peers, and then post one item you’d like to learn.   * Optional Discussion: Comprehensive Certification Readiness (optional and not graded but recommended) located in the Blackboard course shell. | 60  10 |
| 10 | **Data Defenses, Assessments, and Audits**  *ACTIVITIES*   * TestOut Security Pro   + Chapter 9 (Continued): Data * Section 9.7: File Encryption * Section 9.8: Public Key Infrastructure (PKI) * Section 9.9: Hashing * Section 9.10: Data Transmission Security * Section 9.11: Data Loss Prevention (DLP) * Section 9.12: Redundancy * Section 9.13: Backup and Restore * Section 9.14: Cloud Storage   + Section A * Security Pro Practice Exams   + Section B * CompTIA Security+ Practice Exams   *EVALUATION*   * Week 10 TestOut Assessment   *DISCUSS*   * Discussion Question: Your Learning Progress   Post the top three things you learned this week, read and comment to your peers, and then post one item you’d like to learn.   * Optional Discussion: Comprehensive Certification Readiness (optional and not graded but recommended) located in the Blackboard course shell. | 60  10 |
| 11 | **Security Pro Certification Exam**  *EVALUATION*   * TestOut Security Pro Certification Final Exam (200 points)   **Note: Attention Students**: You get only ONE attempt at the final exam. The exam is two hours and must be completed in one sitting. Be sure you are in a quiet place and that you will have sufficient time without any distractions before clicking the link to start the final. Be absolutely certain that you are ready to begin. Once you begin, the clock will start and you will have to complete the exam by the expiration of the time allotted. Do not even click on the link until you are ready to begin the exam. Your instructor cannot “reset” this exam. You have worked very hard on your preparation for this exam, and you should feel confident that if you have been doing your labs and weekly assessments, you will be successful on the final. Believe in yourself as we do at Strayer!  Optional Certification (optional and not graded, but recommended)   * Comprehensive Certification Discussion, located in the Blackboard course shell. * CompTIA Security+ Exam   + Strayer University strives to help IT students obtain recognized industry certifications. Certification, experience, and your degree will help you be most successful in your career. The best time to earn the certification is when all the certification domains are fresh in your mind. You already did most of the work, so there is no point waiting to get your certification. If you’ve consistently done well in your labs, you may feel you are ready for your industry certification exam. Click [here](https://certification.comptia.org/certifications/4-steps-to-certification) to learn about how to prepare to take your CompTIA Security+ Certification Exam.   + We encourage you to take the certification exam as soon as possible on successful completion of this class. Your TestOut access is good for 18 months to help you prepare. Strayer wishes the best for our students. This starts with your certification exam.   *DISCUSS*   * Discussion Question: You plans for taking the CompTIA Certification Exam   You’re almost finished with this course. This week you’ll take the final exam which will test your knowledge about all the topics on the CompTIA Security+ Certification exam.  Take a moment to think about your plans and respond to these items in your post:   * + When do you plan to take the CompTIA certification exam?   + What is one thing you can do to boost your performance on the exam? | 200    0 |

**GRADING SCALE – UNDERGRADUATE**

|  |  |  |
| --- | --- | --- |
| **Assignment** | **Total Points** | **% of**  **Grade** |
| TestOut Weekly Assessment (worth 60 points each)  **Note:** These assessments can be retaken to improve your grade up until the due date. The most recent score will be automatically recorded in the Blackboard Grade Center. | 600 | 60% |
| Writing Assignment: Creating and Communicating a Security Strategy | 100 | 10% |
| Final Exam  **Note:** This exam may only be taken once. Grades must be transferred manually to the Bb Grade Center by your instructor, so the grade may take a few days to appear. | 200 | 20% |
| Discussion Questions (10 questions, worth 10 points each week) | 100 | 10% |
| Extra Credit for Early and Quality Discussion Participation (worth 5 points each week, at the discretion of the instructor) | 55 |  |
| Totals | 1,000-1,055 | 100% |

|  |  |  |
| --- | --- | --- |
| **Points** | **Percentage** | **Grade** |
| 900 – 1,050 | 90% – 105% | A |
| 800 – 899 | 80% – 89% | B |
| 700 – 799 | 70% – 79% | C |
| 600 – 699 | 60% – 69% | D |
| Below 600 | Below 60% | F |

**ATTENDANCE POLICY**

This course uses the TestOut platform for all course content and lab work. However, attendance each week is tracked through your activity in the discussions. Make sure to post an initial response early in the week (by Wednesday) and reply to other students in your discussion each week to receive credit for attendance. Bonus points will be awarded at the instructor’s discretion for early and quality discussion participation.

**WRITING ASSIGNMENTS**

The objective of the School of Information Systems’ writing assignments is to promote attitudes and skills that will improve a student’s ability to communicate in writing, develop research skills and documentation techniques, and encourage critical analysis of data and conclusions specific to the course learning outcomes in the information systems and technology domain.

**Assignment 1: Creating and Communicating a Security Strategy**

**First Draft Due Week 4**

**Final Due Week 6, worth 80 points**

As an IT professional, you’ll often be required to communicate policies, standards, and practices in the workplace. For this assignment, you’ll practice this important task by taking on the role of an IT professional charged with creating a memo to communicate your company’s new security strategy.

The specific course learning outcomes associated with this assignment are:

* Analyze the importance of network architecture to security operations.
* Apply information security standards to real-world implementation.
* Communicate how problem-solving concepts are applied in a business environment.
* Use information resources to research issues in information systems security.
* Write clearly about network security topics using proper writing mechanics and business formats.

**Preparation**

1. **Review the essential elements of a security strategy**

A successful IT administration strategy requires the continuous enforcement of policies, standards, and practices (procedures) within the organization. Review these elements to see how they compare:

|  |  |
| --- | --- |
| **Policy** | The general statements that direct the organization’s internal and external communication and goals. |
| **Standards** | Describe the requirements of a given activity related to the policy. They are more detailed and specific than policies. In effect, standards are rules that evaluate the quality of the activity. For example, standards define the structure of the password and the numbers, letters, and special characters that must be used in order to create a password. |
| **Practices** | The written instructions that describe a series of steps to be followed during the performance of a given activity. Practices must support and enhance the work environment. Also referred to as procedures. |

1. **Describe the business environment**

You are the IT professional in charge of security for a company that has recently opened within a shopping mall. Describe the current IT environment at this business. You can draw details from a company you work for now or for which you have worked in the past. You’ll need to get creative and identify the details about this business that will influence the policies you’ll create. For example, does the company allow cell phone email apps? Does the company allow web mail? If so, how will this affect the mobile computing policy? Describe all the details about this business environment that will be necessary to support your strategy.

1. **Research sample policies**

Familiarize yourself with various templates and sample policies used in the IT field. Do not just copy another company’s security policy, but rather learn from the best practices of other companies and apply them to yours. Use these resources to help structure your policies:

* [Information Security Policy Templates](https://www.sans.org/security-resources/policies)
* [Sample Data Security Policies](https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en)
* [Additional Examples and Tips](#AdditionalExamplesTips)

**Instructions**

With the description of the business environment (the fictional company that has opened in a shopping mall) in mind and your policy review and research complete, create a new security strategy in the format of a company memo (no less than three to five pages) in which you do the following:

1. **Describe the business environment and identify the risk and reasoning**Provide a brief description of all the important areas of the business environment that you’ve discovered in your research. Be sure to identify the reasons that prompted the need to create a security policy.
2. **Assemble a security policy**Assemble a security policy or policies for this business. Using the [memo outline](#MemoTemplate) as a guide, collect industry-specific and quality best practices. **In your own words**, formulate your fictional company’s security policy or policies. You may use online resources, the Strayer Library, or other industry-related resources such as the [National Security Agency](http://www.nsa.gov) (NSA) and [Network World](https://www.networkworld.com/category/security/). In a few brief sentences, provide specific information on how your policy will support the business' goal.
3. **Develop standards**Develop the standards that will describe the requirements of a given activity related to the policy. Standards are the in-depth details of the security policy or policies for a business.
4. **Develop practices**

Develop the practices that will be used to ensure the business enforces what is stated in the security policy or policies and standards.

Format your assignment according to the following formatting requirements:

* This course requires use of new [Strayer Writing Standards (SWS)](https://blackboard.strayer.edu/bbcswebdav/institution/STANDARDIZED/StrayerWritingStandards/Strayer_Writing_Standards.pdf). The format is different than other Strayer University courses. Please take a moment to review the SWS documentation for details.
* This course is designed to prepare you for a career in IT. While most Strayer University courses require SWS (essay) format, this course focuses on writing in a business format. Review this resource to learn more about the important features of business writing: [The One Unbreakable Rule in Business Writing](http://libdatab.strayer.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=118683852&site=eds-live&scope=site).
* You may use the provided memo outline as a guide for this assignment, or you may use your own. Get creative and be original! (You should not just copy a memo from another source.) Adapt the strategy you create to your “company” specifically. In the workplace, it will be important to use company standard documents for this type of communication.
* Do not cut and paste someone else’s strategy. Plagiarism detection software will be used to evaluate your submissions.

**Note:** This assignment will be run through SafeAssign plagiarism detection software and an originality report will automatically be sent to the instructor.

**Rubric**

Grading for this assignment will be based on answer quality, logic/organization of the memo, and language and writing skills, using the following rubric.

| **Points: 80** | **Assignment 1: Creating and Communicating a Security Strategy** | | | | |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Unacceptable**  **Below 60% F** | **Meets Minimum Expectations**  **60-69% D** | **Fair**  **70-79% C** | **Proficient**  **80-89% B** | **Exemplary**  **90-100% A** |
| 1. Describe the business and identify the risk and reasoning  Weight: 20% | Does not describe the business and does not submit or incompletely identifies the risk and reasoning. | Insufficiently describes the business.  The risk is unclear and there is not a clear connection to a reason. | Partially describes the business.  The risk is stated but the reasoning needs more supporting details.  More details and a clear connection to the risk would improve this section. | Satisfactorily describes the business.  The risk is identified and the reasoning has some supporting details. | Thoroughly describes the business.  The risk is clearly identified and the reasoning has well-supported detail to connect the risk to the reasoning. |
| 2. Assemble a security policy or policies for the business  Weight: 25% | Does not submit or incompletely assembles a security policy or policies for the business. | The policy is missing major elements and does not communicate how it would support the business goal. | The policy includes some elements and partially indicates how it would support the business’ goal, but was lacking supporting details. | The policy includes most elements and satisfactorily indicates how it would support the business’ goal, but was lacking supporting details. | The policy includes all the necessary elements and clearly indicates how it will support the business’ goal. |
| 3. Develop standards  Weight: 25% | Does not submit or incompletely develops standards. | The standards are not fully developed and do not describe the requirements of the activity. | The standards partially describe some of the requirements of the activity but lack the details necessary to make them complete. | The standards satisfactorily describe many of the requirements of the activity but could use more details. | The standards thoroughly describe all the requirements of the activity and include sound, in-depth details. |
| 4. Develop practices  Weight: 25% | Does not submit or incompletely develops practices. | The practices do not include enough description to ensure the business can enforce what is stated in the policies and standards.  The written instructions do not include steps or enough steps to make them complete. | The practices partially describe how to ensure the business can enforce what is stated in the policies and standards.  The written instructions include some steps, but they could be expanded to make them complete. | The practices satisfactorily address how to ensure the business can enforce what is stated in the policies and standards.  The written instructions include many of the necessary steps, but additional steps and details would improve the instructions. | The practices thoroughly address how to ensure the business can enforce what is stated in the policies and standards.  The written instructions include all the necessary steps and have well-supporting details. |
| 5. Clarity, writing mechanics, and business  formatting require- ments  Weight: 5% | The writing lacks clarity.  Formatting is not appropriate for business. | The writing lacks some clarity.  Formatting is not appropriate for business. | The writing is beginning to show clarity.  Business formatting is partially applied. | The writing is mostly clear and business formatting is apparent.  Some minor adjustments would improve the overall format. | The writing is professional and clear.  The formatting is excellent and aligned with business requirements. |

**Additional Examples and Tips**

**Example 1: XYZ Inc. Company-Wide Employee Password Strategy**

**Policies**

* + All users must have a password.
  + Passwords must be changed every six months.

**Standards**

* + A password must have a minimum of six characters.
  + A password must have a maximum of 12 characters.
  + A password must contain letters, numbers, and special characters other than $.

**Practices-Employee**

* Create a password. The UserID should be an EmployeeID already generated by HR.
* Send a request to create the account to the Information Technology (IT) department.
* User receives a temporary password.
* Users must change their temporary password the first time they log in.

**Example 2: Security Policy and Standards**Password Policy: Passwords are an important part of computer security at your organization. They often serve as the first line of defense in preventing unauthorized access to the organization’s computers and data.

In order to define the password policy, it is important to identify the standards.

1. Multi-factor authentication

2. Password strength standard

3. Password security standards; how to keep the password secure

**Tips and Points to Consider When Identifying Risks or Security Vulnerabilities**

* + Flaws in operating systems due to constant attack by malware
  + Denial of services attacks
  + Employees data theft
  + User set a weak password or password that is easy to guess, such as a birthday or child’s name.
  + User leaves sensitive data on an unlocked, unattended computer
  + Organization allows sensitive data on a laptop that leaves the building
  + Data can be accessed remotely without using proper security

**Memo Outline**



Network Security Associates of Atlantis, Inc.  
123 Watery Lane  
Atlantis, USVI 91199

From: IT Security Dept.  
Re: Security Policy

Date:

Section 1: General Policies and Motivation

Section 2: Passwords

Section 3: Biometrics

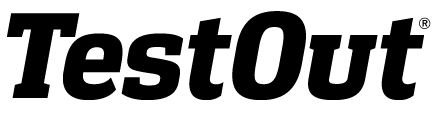
Section 4: Tokens

Section 5: Physical Security

Section 6: Email Policies

Section 7: Breach Reporting Responsibilities

Section 8: Mobile Policy and BYOD (Bring Your Own Device)

****

**Weeks 1 through 10 (60 points per week)**

Students will purchase activation codes for this teaching and simulation platform used throughout this course. They will access this platform through links in their course shell, taking them to each chapter covered in each week. Did you know that by purchasing your TestOut Security Pro activation code from the Strayer University bookstore, you have automatic access to the full Security Pro course for a total of 18 months from the purchase date?

Students should work their way through all the required sections/activities for the week, then return to their Blackboard course shell. Next, they should check the “**Mark Reviewed**” button indicating that they have completed all weekly activities in TestOut. This action will trigger the link to the weekly TestOut Assessment to display. Students should then complete the graded Assessment each week, which measures the knowledge and skills they have learned in each week’s TestOut labs and activities.

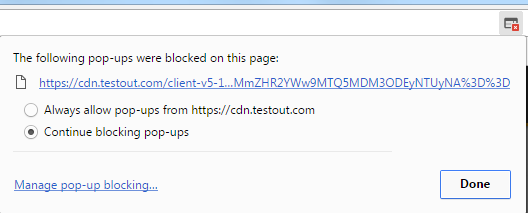
**Note:** For technical assistance with Testout:

* Ask Strayer’s Chat Bot on the iCampus homepage
* Chat with a Live Agent at <https://icampus.strayer.edu/technical-support>
* Submit a Help Ticket at <https://icampus.strayer.edu/technical-support>

**Note:** Google Chrome is the recommended browser to use when accessing TestOut.

**Note**: If you experience any trouble opening the Skills Labs in TestOut (weeks 4 on up), here are a few troubleshooting tips to try:

* Disable the popup blocker in your browser. If you are using Google Chrome, for example, the popup blocker will automatically default on and block the first lab. To view the lab, you must click the icon on the top right of your browser toolbar, then select “Always allow pop-ups from <https://cdn.testout.com>”, then click the Done button.



* Try a different browser and/or clear your cache/history/cookies.

**Security Pro Certification:** After completing all sections of the Security Pro course, you are required to take the TestOut Security Pro Certification as the final exam. Students who pass this final exam with a 68% or higher grade will be awarded the Security Pro Certification by TestOut.

***Attention Students:*** You get only ONE attempt at the final exam, and it must be completed within two hours in one sitting. Be sure you are in a quiet place and that you will have sufficient time without any distractions before clicking the link to start the final. Be absolutely certain that you are ready to begin. Once you begin, the clock will start and you will have to complete the exam by the expiration of the time allotted. Do not even click on the link above until you are ready to begin the exam. Your instructor cannot “reset” this exam. You have worked very hard on your preparation for this exam, and you should feel confident that if you have been doing your labs and weekly assessments, you will be successful on the final. Believe in yourself as we do at Strayer!

On passing the certification exam, you will be prompted to download the certificate of completion. You may also choose to purchase an additional printed copy and/or laminated wallet card from TestOut for a fee.

**Technical Policy**

At Strayer University, a high-quality student education is our number-one goal. To this end, we employ various technology solutions to enhance your experience. With the use of technology, problems can arise from time to time. Therefore, the University has developed the following helpful policy and procedure to support you in getting up and running and back on track as quickly as possible in the event of any technical issue(s).

1. Students must possess or have regular access to computer equipment that is appropriate for their program.

Due to the nature of the technology studied, in IS and IT programs, the best computer to have is a PC with at least a multi-core processor and 1 GB of RAM. Windows 7 or later is also recommended, while some classes may study newer operating systems. It is possible for students to accomplish many classroom tasks with other computers, such as a Chromebook or a Mac, but it is best to have a computer available that meets the minimum system requirements of all the support materials required in program courses. Ultimately, you will save a considerable amount of time troubleshooting issues that could be avoided by acquiring the recommended computer. (NOTE: THESE REQUIREMENTS ONLY RELATE TO THE IS AND IT PROGRAMS.)

1. At the first sign of trouble, students must **communicate, document, and follow through with the appropriate individuals or department**. To avoid last-minute technical issues, students are highly encouraged to start working on their assignments as early in the week as possible. Below are the steps to follow.
2. **Communicate.** 
   1. **Call the helpdesk**. Email: [ithelpdesk@strayer.edu](mailto:ithelpdesk@strayer.edu) Phone: 866.610.8123

* Initial Contact Session with Tech Support:When you speak with a technician, you should be prepared to:
* Thoroughly describe the software you’re working with and your operating system.
* Describe the error message(s) you have gotten and what you have tried to remedy the situation.
* Please call from a quiet place, free from distractions, and have your computer available. The initial call may take some time.

1. **Document.** You should note the name of the technician, the ticket number, and also the time and date of the call. This information should be kept indefinitely, in case the same or similar problem should arise. You may have to give the information to another technician or your instructor.
2. **Follow through.** If the issue is not resolved, you are responsible for following up with the IT technician. A time should be set when you should expect to hear back. If you have not been contacted by the designated time, you should call back. You should have the first contact session information handy and document the new session as well. You should NEVER wait more than 24 hours to have an issue resolved. If you are directed to a third-party vendor for technical support on a particular product, you should document this session in exactly the same way, including the exact phone number called, time, date, technician name, and ticket number. Also, continue to communicate with your instructor about the issue if it persists.

**Now what?** You have contacted, documented, and followed through. If the issue is still not resolved, you should then communicate the documentation you’ve gathered to your instructor. The instructor is the person who most needs to know that you are having a technical issue(s). The instructor will either contact tech support or escalate the issue to the Dean for follow-up. This process can take another 24 hours, so the importance of students starting work early in the week is essential.

Please note: It’s possible that some issues may not be solvable by Strayer technical support, though this is rare. If the issue is determined to be the student’s equipment or software, the student may be required to secure computer resources which are up to the specifications required.

As long as students are being proactive, communicating, documenting, and following through, their grade will not suffer. Following this resolution model, students will find that issues are solved quickly and they won’t get behind. The key to a smooth student experience is you! The more you invest in your education, the more you will get out of it!