Writing Security: Teaching Security Ethics Through Policy Writing

For Instructors:

Discussion of ethical development and uses of computing have recently increased in technology fields such as computer security. Developing and sharing interdisciplinary course materials may make it easier for instructors to include a broader range of ethical concepts into their technical security courses. This packet connects security and ethics for students by asking them to create a security policy and consider ethical concerns such as systemic inequality and disproportionate harms. This curriculum is particularly well-suited for courses in computer or information security but could be used to discuss ethics in any information or computer science course.

Packet Contents

This packet contains lesson plans for encouraging ethical reflection during a security policy writing exercise using one of three case studies: **COVID-19 Contact Tracing, Network Traffic Monitoring,** and **Exam Proctoring Technologies**.

Each of these three case studies requires two class sessions, and contains a set of unique readings and materials. Each case study contains three modules:

- Module 1 is an assignment that asks students **draft a security policy** that represents the interests of a particular stakeholder group
- Module 2 gives students feedback through either **instructor critique** or a **peer review** assignment.
- Module 3 is an assignment that asks students to **revise their security policy** by integrating critiques and proposing policy alternatives.

Writing Security: Teaching Security Ethics Through Policy Writing

Student Learning Objectives

Students will be able to:

- Recognize how they are ethical agents when practicing computer security
- Foreground conversations of inequality and harms as security ethics issues
- Synthesize feedback and create meaningful security policy alternatives

For Instructors:

To emphasize to students that they themselves are ethical agents when practicing technology security, this packet walks students through the process of creating, critiquing, and revising a security policy. Developing security policies is a common but heterogeneous task for security professionals, spanning both organizational security policies to guide human behavior and technical security policies that guide machine behavior. As such, crafting and problematizing policies is both a critical technology security skill and a key site of ethical practice in technology security work. Our activity both guides students through the policy writing process and calls attention to when ethics are being practiced.

To foreground conversations of ethics in security issues, our activity prompts students to think through power dynamics in stakeholder relations as they create and revise their policy. Our prompts emphasize two concepts borrowed from technology ethics literature: that technologies reproduce patterns of inequality and harm, and that these patterns disproportionally affect specific communities.

Finally, our activity gives students experience in problematizing security policy proposals and responding to feedback with meaningful security policy alternatives. The ability to problematize security policies before they are implemented and respond to problems afterwards is a key skill in technology security practice, making this activity professionally relevant.

Exam Proctoring Technologies: Background and References

Background

Universities and schools increasingly use **remote exam proctoring technologies** developed by private companies, such as Proctorio, Examity, HonorLock, or ProctorU. While these companies claim remote exam proctoring technologies reduce cheating during online tests, the invasiveness of the surveillance techniques involved creates both security and ethical concerns. These concerns can be particularly salient for those from marginalized communities, since technologies often reproduce patterns of inequality and harm.

In this exercise, we will examine how security and ethics are tied together by creating a *security policy*. These policies help organizations operationalize their security practices by describing who and what is to be protected, and from whom; protocols for when threats are detected; and enforcement procedures for ensuring security.

Required Readings

Lawson, Sean (2020, April 24). **"Are Schools Forcing Students To Install Spyware That Invades Their Privacy As A Result Of The Coronavirus Lockdown?".** *Forbes.* https://www.forbes.com/sites/seanlawson/2020/04/24/are-schools-forcing-students-to-install-spyware-that-invades-their-privacy-as-a-result-of-the-coronavirus-lockdown/

Diwan, Fahad (2021, Jan 29). **"University Will Stop Using Controversial Remote-Testing Software Following Student Outcry".** *The Verge.* https://www.theverge.com/2021/1/28/22254631/university-of-illinois-urbana-champaign-proctorio-online-test-proctoring-privacy

Swauger, Shea (2020, April 2). **"Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education".** *Hybrid Pedagogy.* https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/

Left image credit: https://www.sheffield.ac.uk/polopoly_fs/1.728754!/image/seminar.png

Right image credit: https://en.wikipedia.org/wiki/Panopticon#/media/File:Panopticon.jpg

Exam Proctoring Technologies: Drafting a Security Policy

Group Assignment

Complete the required readings, keeping track of what data exam proctoring technologies capture and how, where data is stored, who has access to data, and how remote proctoring technologies might be more concerning for specific groups of people. Now imagine that your school wants to understand both the security and ethical implications of using Proctorio. Your school's administration has asked a variety of stakeholders to draft a security policy that reflects their specific needs and concerns.

Select and Analyze a Stakeholder Group

Select a specific entity with a vested interest in your school's security policy for Proctorio. This **must be someone other than "students"**, such as:

- Instructors who will use Proctorio
- A school's disability services department, such as the University of Washington's Disability Resources for Students.
- A school office that supports victims of sexual harassment or domestic violence
- A student group that represents the interests of undocumented students, such as UW's Leadership Without Borders.
- Parents or guardians of students

Do a small amount of research on your chosen stakeholder group. You might look at a group's mission statement, website, or social media accounts. Next, consider some ethical concerns concerning your stakeholder by answering the following questions:

- What goals or concerns might your stakeholder group have about Proctorio?
- What power does your stakeholder group have over Proctorio at your school?
- What other stakeholder groups might have similar interests?
- What other stakeholder groups might have divergent or conflicting interests?
- What system abuses might be particularly concerning to your stakeholder group?
- What data or procedures involved in Proctorio might be particularly or uniquely concerning for your stakeholder group?

Group Assignment: Drafting a Security Policy (continued)

Now that your group has selected and analyzed a stakeholder group, answer the following questions to begin drafting your stakeholder's security policy.

Drafting Security Policy Sections

Acceptable use - What student devices can Proctorio access or require? How can student data be used? Are any procedures or uses restricted? Is Proctorio allowed to gather any other data (e.g., social media data)?

Data access - Once created, who should have access to student data, and under what conditions? What about employees of Proctorio?

Security incidents - Who is likely to want to breach or gain access to student data? What should happen in the event the system is abused or breached?

Special protections - Are there types of student data or groups of students who should have special protections? If so, how should they be implemented?

Data retention - How should student data be kept? For how long? By whom? Are there any exceptions?

Remediation - How are conflicts, problems, or flaws resolved (e.g., a student who does not have a webcam or other required device)?

Compliance - Who verifies that the rules in the policy are being followed? What are the penalties for security breaches, data misuse, and other noncompliance?

What To Submit

Synthesize your work into a security policy (1000 - 1500 words) that you believe represents your stakholder's interests. Your group's security policy should have a section for each of the seven categories above.

Tip: If you are having trouble getting started, the SANS Institute has a number of security policy templates. In particular, pay attention to the Policy sections: https://www.sans.org/information-security-policy/

Exam Proctoring Technologies: Peer Review

Peer Review Assignment

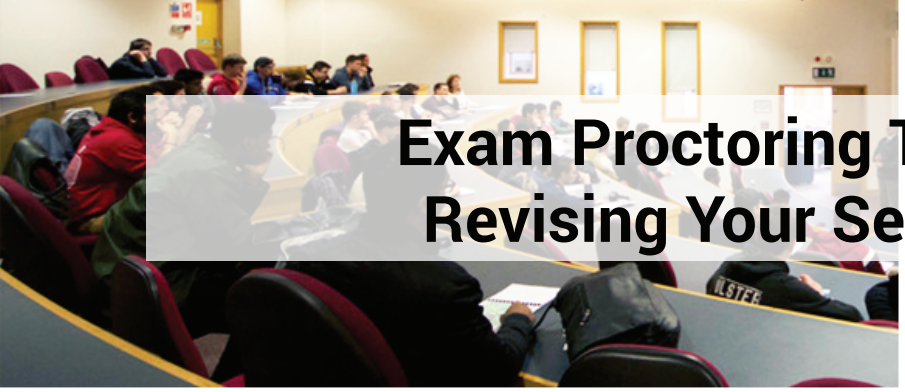
Giving constructive feedback is a skill that takes both guided practice and time. For this assignment, you will individually peer review a different group's security policy. To help you write a great peer review, we have provided some scaffolding questions for thinking about the security and ethical implications of a group's security policy. You do not have to submit your answers to these questions, these are just to get you started:

- Does the security policy account for all the ways Proctorio can monitor students?
- Whose needs are being met? At whose expense are these needs being met?
- Are the needs of your stakeholder group being met?
- Would your stakeholder group object to anything?
- Are any of the security policy's exceptions or protections concerning for your stakeholder group?
- Are the obligations placed on different stakeholders achievable? Are the obligations reasonable?
- Are there any foreseeable conflicts that the policy does not address?

What To Submit

Synthesize your feedback into a 500 - 600 word peer review. You should answer the following questions directly in your peer review:

- What did you think was the best part of this group's security policy?
- Where was this group's security policy clear?
- Where did you get confused?
- Do you think this group overlooked or missed something that might make their security policy more complete?



Exam Proctoring Technologies: Revising Your Security Policy

Group Assignment

Your group has received feedback on your draft security policy. Your next step is to integrate this feedback into a finalized security policy.

Each group member should individually and independently identify at least three (3) points from your critique that are interesting, complicate your draft security policy, or make you want to change your draft. For each point, write down:

- What was the critique?
- Why has this critique made you consider changing your security policy?
- How do you think you should amend your security policy?

Synthesize these thoughts into an individual 500 word reflection document.

Discuss your reflections with your group. When discussing your reflections with your group members, you may find disagreements, inconsistencies, blind spots, or other items which will require negotiation between group members. We also ask you to **document your group's negotiation process**. Record agreements, disagreements, and reconciliations into a separate document. There is no minimum word limit for this, but try to be as thorough as you can.

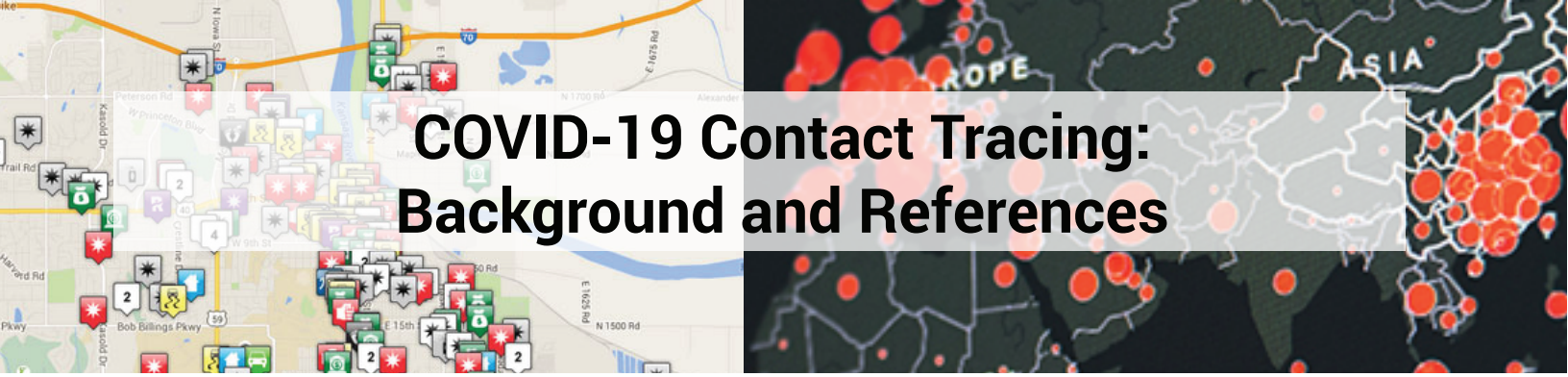
After negotiating your policy changes, synthesize your collected reflections into a finalized security policy to govern Proctorio at your school. **A comprehensive security policy will be about 2000 words**.

What To Submit

Each group should submit:

- Your group's initial security policy (1000 - 1500 words)
- Each group members feedback reflection document (500 words each)
- Your group's final security policy (~2000 words)
- Documentation of your group's process of negotiating and implementing changes to the policy

One group member is responsible for submitting all documents.



COVID-19 Contact Tracing: Background and References

Background

The COVID-19 pandemic created an urgent need for **contact tracing**. Contact tracing involves identifying and notifying people who may have been exposed to a known infected individual. In manual contact tracing, patients are asked where they have been recently, with whom, and when. Automating this process using cell phone applications has the potential to improve accuracy and speed, helping to "flatten the curve". While contact tracing apps seem promising, such tracing also creates security and ethical concerns. These concerns can be particularly salient for those from marginalized communities, since technologies often reproduce patterns of inequality and harm.

In this exercise, we will examine how security and ethics are tied together by creating a *security policy*. These policies help organizations operationalize their security practices by describing who and what is to be protected, and from whom; protocols for when threats are detected; and enforcement procedures for ensuring security.

Required Readings

Gray, Stacey (2020, March 25). **"A Closer Look at Location Data: Privacy and Pandemics".** *Future of Privacy Forum*. https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/

Crocker, Andrew. Opsahl, Kurt. Cyphers, Bennett (2020, April 10). **"The Challenge of Proximity Apps for COVID-19 Contact Tracing".** *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

Toh, Amos. Brown, Deborah (2020, June 4). **"How Digital Contact Tracing for COVID-19 Could Worsen Inequality".** *Human Rights Watch - Just Security.* https://www.hrw.org/news/2020/06/04/how-digital-contact-tracing-covid-19-could-worsen-inequality

Left image credit: https://lawrenceks.org/police/crime-map/

Right image credit: https://sph.umich.edu/news/2020posts/surveillance-testing-gathering-the-data-on-covid-19.html

COVID-19 Contact Tracing: Drafting a Security Policy

Group Assignment

Complete the required readings, keeping track of what data contact tracing technologies capture, how contact data is combined with other data, who has access to data, and how contact tracing might be more concerning for specific groups of people. Now imagine that your school wants to understand both the security and ethical implications of deploying a campus-wide contact tracing app. Your school's administration has asked a variety of stakeholders to draft a security policy that reflects their needs and concerns.

Select and Analyze a Stakeholder Group

Select a specific entity with a vested interest in your school's security policy for a campus contact tracing app. This **must be someone other than "students"**, such as:

- A local University's epidemiology department or a hospital.
- A school office that supports victims of sexual harassment or domestic violence
- A student group that represents the interests of campus diversity and inclusion, such as the University of Washington's Women in Science and Engineering.
- Your school's Information Technology (IT) department.
- A student group that represents the interests of undocumented students, such as the UW's Leadership Without Borders.

Do a small amount of research on your chosen stakeholder group. You might look at a group's mission statement, website, or social media accounts. Next, consider some ethical concerns concerning your stakeholder by answering the following questions:

- What goals or concerns might your stakeholder group have about contact tracing?
- What power does your stakeholder group have over contact tracing at your school?
- What other stakeholder groups might have similar interests?
- What other stakeholder groups might have divergent or conflicting interests?
- What system abuses might be particularly concerning to your stakeholder group?
- What data or procedures involved in contact tracing might be particularly or uniquely concerning for your stakeholder group?

Group Assignment: Drafting a Security Policy (continued)

Now that your group has selected and analyzed a stakeholder group, answer the following questions to begin drafting your stakeholder's security policy.

Drafting Security Policy Sections

Acceptable use - Should there be limits on what data is captured or how it is used? Are there limits on combining other data (e.g. social media) with contact tracing data?

Data access - Who should have access to contact tracing data, and under what conditions? Should data be made public? If so, how?

Security incidents - Who is likely to want to breach or gain access to your school's contact tracing data? What should happen in the event of an intrusion or breach?

Special protections - Are there types of data or groups of people that should have special protections? If so, what should those protections be? How will these protections be implemented?

Data retention - How should network data be kept? For how long? By whom? Are there any exceptions?

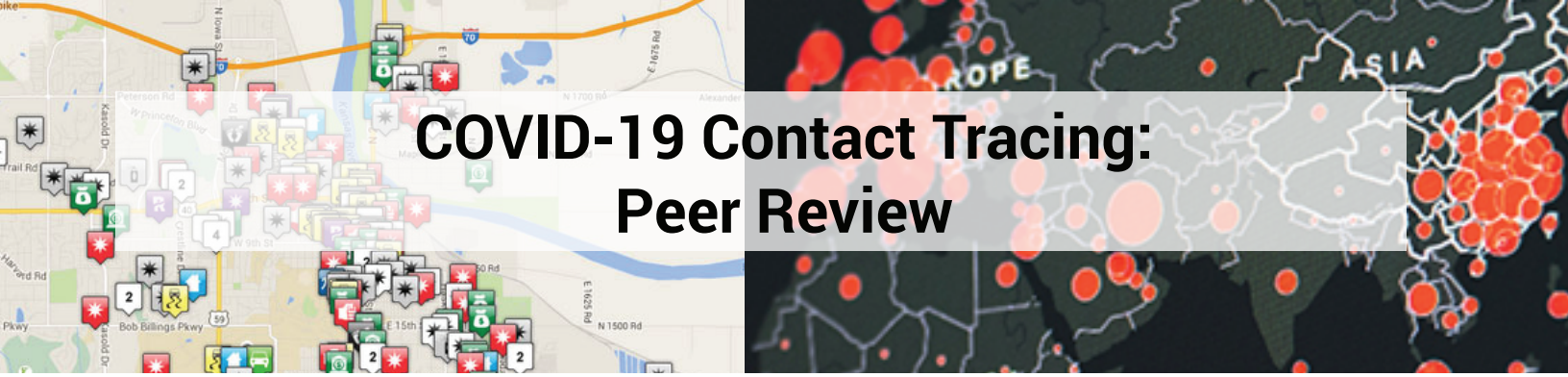
Remediation - How are conflicts, problems, or flaws resolved (e.g., discovering a vulnerability in a database holding contact tracing data)?

Compliance - Who verifies that the rules in the policy are being followed? What are the penalties for security breaches, data misuse, and other noncompliance?

What To Submit

Synthesize your work into a security policy (1000 - 1500 words) that you believe represents your stakholder's interests. Your group's security policy should have a section for each of the seven categories above.

Tip: If you are having trouble getting started, the SANS Institute has a number of security policy templates. In particular, pay attention to the Policy sections: https://www.sans.org/information-security-policy/



COVID-19 Contact Tracing: Peer Review

Peer Review Assignment

Giving constructive feedback is a skill that takes both guided practice and time. For this assignment, you will individually peer review a different group's security policy. To help you write a great peer review, we have provided some scaffolding questions for thinking about the security and ethical implications of a group's security policy. You do not have to submit your answers to these questions, these are just to get you started:

- Does the security policy account for all the ways contact tracing can monitor people?
- Whose needs are being met? At whose expense are these needs being met?
- Are the needs of your stakeholder group being met?
- Would your stakeholder group object to anything?
- Are any of the security policy's exceptions or protections concerning for your stakeholder group?
- Are the obligations placed on different stakeholders achievable? Are the obligations reasonable?
- Are there any foreseeable conflicts that the policy does not address?

What To Submit

Synthesize your feedback into a 500 - 600 word peer review. You should answer the following questions directly in your peer review:

- What did you think was the best part of this group's security policy?
- Where was this group's security policy clear?
- Where did you get confused?
- Do you think this group overlooked or missed something that might make their security policy more complete?

COVID-19 Contact Tracing: Revising Your Security Policy

Group Assignment

Your group has received feedback on your draft security policy. Your next step is to integrate this feedback into a finalized security policy.

Each group member should individually and independently identify at least three (3) points from your critique that are interesting, complicate your draft security policy, or make you want to change your draft. For each point, write down:

- What was the critique?
- Why has this critique made you consider changing your security policy?
- How do you think you should amend your security policy?

Synthesize these thoughts into an individual 500 word reflection document.

Discuss your reflections with your group. When discussing your reflections with your group members, you may find disagreements, inconsistencies, blind spots, or other items which will require negotiation between group members. We also ask you to **document your group's negotiation process**. Record agreements, disagreements, and reconciliations into a separate document. There is no minimum word limit for this, but try to be as thorough as you can.

After negotiating your policy changes, synthesize your collected reflections into a finalized security policy for your school's contact tracing app. **A comprehensive security policy will be about 2000 words**.

What To Submit

Each group should submit:

- Your group's initial security policy (1000 - 1500 words)
- Each group members feedback reflection document (500 words each)
- Your group's final security policy (~2000 words)
- Documentation of your group's process of negotiating and implementing changes to the policy

One group member is responsible for submitting all documents.

Network Traffic Monitoring: Background and References

Background

As networked devices like cell phones and Internet of Things (IoT) proliferate, so does their network footprint. Increases in the volume and variety of network traffic make it difficult to quickly detect and respond to potential network intrusions. While **network traffic monitoring** can improve network intrusion detection and response by recording network traffic metadata at routers, switches, and other network devices, this capacity for surveillance also creates security and ethical concerns. These concerns can be particularly salient for those from marginalized communities, since technologies often reproduce patterns of inequality and harm.

In this exercise, we will examine how security and ethics are tied together by creating a *security policy*. These policies help organizations operationalize their security practices by describing who and what is to be protected, and from whom; protocols for when threats are detected; and enforcement procedures for ensuring security.

Required Readings

Shimeall, Tim (2016, September 16). **"Traffic Analysis for Network Security: Two Approaches for Going Beyond Network Flow".** *Software Engineering Institute, CMU*. https://insights.sei.cmu.edu/sei_blog/2016/09/traffic-analysis-for-network-security-two-approaches-for-going-beyond-network-flow-data.html

Crocker, Andrew. Opsahl, Kurt. Cyphers, Bennett (2020, April 10). **"The Challenge of Proximity Apps for COVID-19 Contact Tracing".** *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

Gray, Stacey (2020, March 25). **"A Closer Look at Location Data: Privacy and Pandemics".** *Future of Privacy Forum*. https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/

Left image credit: https://www.scnsoft.com/blog/detecting-apt-activity-with-network-traffic-analysis

Right image credit: https://tcf.org/content/report/disparate-impact-surveillance/

Network Traffic Monitoring: Drafting a Security Policy

Group Assignment

Complete the required readings, keeping track of why monitoring network traffic is useful, what data and devices are involved, how network data can be combined with other data, and how network monitoring may be more concerning for specific groups of people. Now imagine that your school wants to understand both the security and ethical implications of their network monitoring practices. They have asked a variety of stakeholders to draft a security policy that reflects their needs and concerns.

Select and Analyze a Stakeholder Group

Select a specific entity with a vested interest in your school's security policy for network traffic analysis. This **must be someone other than "students"**, such as:

- School employees (e.g., teachers, administrators, janitors, or contractors)
- A school office that supports victims of sexual harassment or domestic violence
- A student group that represents the interests of campus diversity and inclusion, such as the University of Washington's Women in Science and Engineering.
- A student group that represents the interests of undocumented students, such as the UW's Leadership Without Borders.
- Your school's Information Technology (IT) department

Do a small amount of research on your chosen stakeholder group. You might look at a group's mission statement, website, or social media accounts. Next, consider some ethical concerns concerning your stakeholder by answering the following questions:

- What goals or concerns might your stakeholder group have about network traffic monitoring?
- What power does your stakeholder group have over network monitoring at your school?
- What other stakeholder groups might have similar interests?
- What other stakeholder groups might have divergent or conflicting interests?
- What system abuses might be particularly concerning to your stakeholder group?
- What data or procedures involved in network traffic monitoring might be uniquely concerning for your stakeholder group?

Group Assignment: Drafting a Security Policy (continued)

Now that your group has selected and analyzed a stakeholder group, answer the following questions to begin drafting your stakeholder's security policy.

Drafting Security Policy Sections

Acceptable use - Should there be limits on what network data is captured or how it is used? Are there limits on combining other data (e.g. social media) with network data?

Data access - Who should have access to network data, and under what conditions? When is it okay to share network data (e.g., with researchers, law enforcement)?

Security incidents - What should happen in the event of an intrusion or breach? Who might want to breach or gain access to your school's network data?

Special protections - Are there types of network data or groups of people that should have special protections? If so, what should those protections be? How will these protections be implemented?

Data retention - How should network data be stored? For how long? By whom? Are there any exceptions? Who or what decides when data is deleted forever?

Remediation - How are conflicts, problems, or flaws resolved (e.g., a court order for a school's network data)?

Compliance - Who verifies that the rules in the policy are being followed? What are the penalties for security breaches, data misuse, and other noncompliance?

What To Submit

Synthesize your work into a security policy (1000 - 1500 words) that you believe represents your stakholder's interests. Your group's security policy should have a section for each of the seven categories above.

Tip: If you are having trouble getting started, the SANS Institute has a number of security policy templates. In particular, pay attention to the Policy sections: https://www.sans.org/information-security-policy/

Network Traffic Monitoring: Peer Review

Peer Review Assignment

Giving constructive feedback is a skill that takes both guided practice and time. For this assignment, you will individually peer review a different group's security policy. To help you write a great peer review, we have provided some scaffolding questions for thinking about the security and ethical implications of a group's security policy. You do not have to submit your answers to these questions, these are just to get you started:

- Does the security policy account for all the ways network traffic can be monitored?
- Whose needs are being met? At whose expense are these needs being met?
- Are the needs of your stakeholder group being met?
- Would your stakeholder group object to anything?
- Are any of the security policy's exceptions or protections concerning for your stakeholder group?
- Are the obligations placed on different stakeholders achievable? Are the obligations reasonable?
- Are there any foreseeable conflicts that the policy does not address?

What To Submit

Synthesize your feedback into a 500 - 600 word peer review. You should answer the following questions directly in your peer review:

- What did you think was the best part of this group's security policy?
- Where was this group's security policy clear?
- Where did you get confused?
- Do you think this group overlooked or missed something that might make their security policy more complete?

Exam Proctoring Technologies: Revising Your Security Policy

Group Assignment

Your group has received feedback on your draft security policy. Your next step is to integrate this feedback into a finalized security policy.

Each group member should individually and independently identify at least three (3) points from your critique that are interesting, complicate your draft security policy, or make you want to change your draft. For each point, write down:

- What was the critique?
- Why has this critique made you consider changing your security policy?
- How do you think you should amend your security policy?

Synthesize these thoughts into an individual 500 word reflection document.

Discuss your reflections with your group. When discussing your reflections with your group members, you may find disagreements, inconsistencies, blind spots, or other items which will require negotiation between group members. We also ask you to **document your group's negotiation process**. Record agreements, disagreements, and reconciliations into a separate document. There is no minimum word limit for this, but try to be as thorough as you can.

After negotiating your policy changes, synthesize your collected reflections into a finalized security policy for your school's network traffic monitoring practices. **A comprehensive security policy will be about 2000 words**.

What To Submit

Each group should submit:

- Your group's initial security policy (1000 - 1500 words)
- Each group members feedback reflection document (500 words each)
- Your group's final security policy (~2000 words)
- Documentation of your group's process of negotiating and implementing changes to the policy

One group member is responsible for submitting all documents.