CYBR 3321 Assignments:

\*\*\*NOTE: THIS WAS PART OF THE PLANNING FOR THE COURSE\*\*\*

1. For Week of: 2/8 Government Regulations of Internet

Assignment Name: COPPA-Compliant AUP

NICE Framework – Oversee & Govern – Strategic Planning & Policy – Cyber Policy & Strategy Planner

T0408

As a company that makes mobile app games for kids, we are required to adhere to COPPA. As our Cyber Policy & Strategy Planner, we need you to draft an acceptable use policy for users of our game as the demographic is largely kids under 13.

You can start here: <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business>

Work with your team and build an acceptable usage policy that is COPPA-compliant. Once completed, submit your AUP as well as an additional document on actionable steps our developers need to do to ensure our mobile games are COPPA compliant as well.

Additional Resources:

<https://www.dwt.com/blogs/family-business-resource-center/2022/02/how-to-comply-with-coppa>

<https://www.iubenda.com/en/help/113898-coppa-compliance-checklist>

Deliverables: **COPPA-Compliant AUP in PDF Format**

Rubric:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criteria** | **Excellent (25)** | **Good (15)** | **Satisfactory (10)** | **Needs Improvement (5)** |
| **Information** | Comprehensive and accurate coverage of all relevant COPPA requirements, with detailed explanations and relevant examples. | Accurate coverage of most COPPA requirements, with some minor areas lacking detail or examples. | Basic coverage of key COPPA requirements, but some important aspects are missing or underdeveloped. | Significant inaccuracies or omissions in COPPA-related information, lacking depth and detail. |
| **COPPA Compliance** | AUP and developer action plan fully compliant with all aspects of COPPA, demonstrating an understanding of the law's implications for children's privacy. | AUP and developer action plans are mostly compliant, with minor gaps in addressing some COPPA aspects. | AUP and developer action plans meet basic COPPA compliance but lack comprehensive coverage of all requirements. | Non-compliance with several aspects of COPPA, missing key requirements of the law. |
| **Clarity and Format** | Well-structured and presented; clear, concise language; logical flow; professional and user-friendly format. | Well-organized with clear language; minor issues in flow or format, but overall easy to understand. | Somewhat organized, but issues with clarity or format affect readability and comprehension. | Poor organization, unclear language, and formatting issues make the document difficult to follow. |
| **Actionable Steps for Developers** | Provides a detailed, practical, and clear action plan for developers to ensure COPPA compliance, with specific steps and examples. | Good action plan with clear steps for developers, but may lack some detail or practical examples. | Basic action plan is provided, but the steps are somewhat vague or lacking in practical guidance. | Incomplete or unclear action plan, lacking specific steps or practical applicability for developers. |

Due: 2/18

1. For Week of 2/22 The Role of the 1st Amendment in Cyber

Assignment Name: GDPR vs. Jurisdiction

NICE Framework – Oversee & Govern – Legal Advice & Advocacy – Privacy Officer/Privacy Compliance Manager

T0913

A complaint has come in concerning our organization’s privacy policies and procedures. An employee believes that our current privacy policy violates GDPR. Recently expanding into the EU, the company felt the privacy policy was solid already. They reasoned that although they offered service to the EU, the data itself was not stored in the EU and thus should fall under the jurisdiction of the US. The employee’s complaint stated that GDPR requires explicit consent, data protection measures, and rights to the data subjects these are not present in the current privacy policy.

The company does not deny this but believes that paying the fine won’t be a bad alternative to quiet the noise being made by this employee. Word of this has spread out and the company production has taken a hit. They are looking to you and your team as Privacy Officers to research and reach out to external legal counsel for additional insight and guidance on the best way to approach this.

Within a few weeks, we need a professional, APA-formatted report that highlights the issue between the company and the employee, summarizes your conclusions as well as the input from the external party, and finally, gives our organization a way to move forward past this…what do we need to do to get back to normal?

Deliverables: **Legal Recommendation Report in PDF Format**

Rubric:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criteria** | **Excellent (25)** | **Good (15)** | **Satisfactory (10)** | **Needs Improvement (5)** |
| **Information** | Comprehensive coverage of GDPR requirements and detailed analysis of the company's policy gaps. Accurately highlights the issue and employee's concerns. | Accurate coverage of most GDPR requirements, good analysis of company policy with minor details missing. | Basic coverage of GDPR and policy analysis, but lacks depth in highlighting specific issues or employee concerns. | Significant inaccuracies or omissions in understanding GDPR and analyzing company policy. |
| **External Consulting** | Insightful input from external legal counsel is included. | Good input from external legal counsel with some valuable insights, but may lack depth in certain areas. | Basic input from external legal counsel included, but lacks comprehensiveness or critical insights. | Missing input from external legal counsel |
| **Format** | Well-written, clear, and concise. Adheres to APA format with proper citations and references. | Well-written with minor errors in clarity or APA format. Generally adheres to academic standards. | Satisfactory writing and adherence to APA format, but with several errors or inconsistencies. | Poorly written with significant issues in clarity, structure, and APA formatting. |
| **Actionable Steps** | Provides a detailed, practical, and clear action plan for addressing the GDPR compliance issue and moving forward. | Good action plan with clear steps, but missing some detail or specificity in addressing the compliance issue. | Basic action plan provided, but steps are somewhat vague or lacking in practical guidance. | Incomplete or unclear action plan, lacking specific steps or practical applicability for resolving the issue. |

Due: 3/10

1. For Week of 3/26 Open Source Software

Assignment Name: (Miniature)Tough on Decision

NICE Framework – Oversee & Govern – Executive Cyber Leadership

T0248

For security and to save costs, your organization has decided to switch to more open-source software, particularly for office apps (think Word, Excel, PowerPoint, etc.). While it may be a learning curve, the IT department has recommended this change as our previous, MinitureTough, had 3 0-days that gave admin remote access (terminal & GUI) to the devices it was installed on. It has even been used to deploy ransomware in several businesses in the Northwest after it’s update server was hacked to deploy it (our security software caught it). After a few weeks of discussing the vulnerabilities with the company, the company alluded to the fact that they knew it was there, they’ve always known it was there and they will never, nor do they have plans to EVER, patch those issues. The board, a bit stuck in their ways, refuses to move away from MinitureTough, they believe the loss of production to be on lazy new hires (plus the old software is what they know).

Your task, as a team of C-Suite Executives, is to not only promote the open-source software (of your choice) but to bring the other security issues to the board's attention. With your team, you are to research open-source office suites that could be used in the organization. Inform the board of MinitureTough’s refusal to fix their software and the threat this poses to the company. Finally, give some actionable steps and encourage the board to take cybersecurity a bit more seriously.

Your challenge is the board only listens to reason and professionalism. They like to hear related studies, evidence, and events to support one’s point. They also won’t be budged by recommendations without some form of support or recognized practice.

They’ve approved you for a 10-minute presentation on the matter, ideally with 5-7 slides. Be sure to have your support ready, they may have questions.

Deliverables: **Presentation (And Presenting in Class)**

Rubric:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criteria** | **Excellent (50)** | **Good (25)** | **Satisfactory (15)** | **Needs Improvement (10)** |
| **Information** | Provides highly accurate and comprehensive information about open-source office suites and security vulnerabilities of MinitureTough. | Information is mostly accurate, with minor errors or omissions about software features or security issues. | Provides basic information but lacks depth or has several inaccuracies. | Significant inaccuracies or lack of detail in describing software options or security risks. |
| **Presentation of Findings** | Clear and organized presentation. Highlights the benefits of open-source software and the risks of MinitureTough. | Well-structured presentation with minor issues in organization or clarity. Communicates most key points. | Decently structured presentation but lacks clarity or cohesion in conveying key findings. | Poorly organized or unclear presentation, fails to communicate key points. |
| **Supporting Arguments** | Provides strong, supporting arguments with relevant studies, evidence, and real-world events. Addresses potential board concerns. | Good supporting arguments with some relevant evidence and examples, but missing depth | Basic supporting arguments provided, but lacks evidence or relevance to board concerns. | Weak or insufficient supporting arguments, with little to no evidence or examples. |
| **Format and Professionalism** | Professional and visually appealing format. Adheres to the 5-7 slide limit and uses the 10-minute presentation time. | Mostly professional format with minor issues. Mostly adheres to slide limit and presentation time. | Satisfactory format, but could be more professional. Some issues with adhering to slide limit or presentation time. | Unprofessional format, exceeds slide limit, or poorly manages presentation time. |

Due: 4/7

1. For Week of 4/4 Workplace Privacy

Assignment Name: When the Workplace goes Home

NICE Framework – Oversee & Govern – Cybersecurity Management – Information Systems Security Manager

T0227

Alt: NICE Framework – Oversee & Govern – Strategic Planning & Policy - Cyber Workforce Developer & Manager

T0387

At a small company of 5 employees (not counting yourself) you work as an Information Systems Security Manager. In fact, you are the only person not a typical employee at this small business (meaning your job is cybersecurity, everyone else’s job is not technology). With COVID, the business had to decide whether or not to stay on site or WFH. They voted unanimously to WFH (except for the owner). The company deals with data processing for local government needs and has quite a few contracts, so the concern of the business is not closing its doors during this difficult time…it’s about where the workplace is.

The owner, believes that if you are taking work home, there should be some form of accountability. He doesn’t like the word spyware but he likes the ability to know what his employees will be doing during work hours.

The 4 employees believe that anything beyond an occasional email and/or call is an invasion of privacy.

The owner refers to the Workplace Privacy Policy:

At Trinity Data, we are committed to respecting the privacy of our employees and maintaining a workplace that ensures confidentiality and protection of personal information. This policy outlines our practices regarding the collection, use, and protection of personal information within our workplace.

Trinity Data Workplace Privacy Policy

**Scope**

This policy applies to all employees, contractors, and visitors of Trinity Data and covers all workplace operations and activities.

**Data Collection**

* We collect personal information necessary for employment purposes, including but not limited to, name, contact information, identification numbers, employment history, and bank details for payroll purposes.
* We may monitor and record activities in the workplace, including phone and internet usage, and access to our network for security and operational purposes.

**Data Use**

* Personal information is used strictly for legitimate business purposes such as payroll processing, benefit administration, performance evaluations, and compliance with legal obligations.
* Employee monitoring will be conducted lawfully and transparently, respecting the employee’s right to privacy and dignity.

**Data Protection**

* We employ reasonable and appropriate security measures to protect employee information from unauthorized access, disclosure, alteration, or destruction.
* Access to personal information is restricted to authorized personnel who have a legitimate business need to access the information.

**Employee Rights**

* Employees have the right to access their personal information held by the company and may request corrections or updates to ensure accuracy.
* Employees may request information about the processing of their personal data and the rationale behind any monitoring activities.

**Confidentiality of Employee Information**

* Personal information of employees is considered confidential and will not be disclosed to third parties without consent unless required by law.

**Policy Compliance**

* Employees are expected to comply with this policy and to safeguard personal information pertaining to their colleagues.
* Any breaches of this privacy policy will be taken seriously and may result in disciplinary action.

**Policy Review and Amendments**

* This policy will be reviewed regularly and may be amended to remain compliant with relevant laws and regulations or to reflect changes in our business operations.

**Questions and Concerns**

* Employees who have questions or concerns about any aspect of this policy should contact The Owner.

**Acknowledgment**

* By continuing your employment at Trinity Data, you acknowledge that you have read, understood, and agreed to comply with this Workplace Privacy Policy.

He argues that Data Collection, bullet 2, gives the company the right to monitor, even if their workplace moves home. He promises that it will be done lawfully and transparently as under Data Use, bullet 2. He also reminds them of their employee rights and is open to being transparent about information as it relates to the business.

The employees are not sold on this as data would be collected from inside of the homes and all of their company-issued devices have webcams and microphones built in. They are also a bit unnerved by the owner’s hard stance on this as well. They understand what they signed by don’t believe it should apply given the circumstances or at least an amendment or two should be considered.

The owner disagrees. They all look to you for guidance.

Review the arguments and stances. As well as the workplace privacy policy. How would you resolve this issue? Would you recommend alternatives? Or do you side with one side or the other?

Once you conclude, create a 1-2 page APA formatted report that outlines the issue, your recommendation, and how it resolves the conflict. Be sure to reference the facts as given and any outside sources that you may have used.

Deliverables: **Resolution Report in PDF Format**

Rubric:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criteria** | **Excellent (25)** | **Good (15)** | **Satisfactory (10)** | **Needs Improvement (5)** |
| **Information** | Provides highly accurate and comprehensive information regarding the privacy policy, employee concerns, and legal implications. | Accurately presents most information but may miss some minor details. | Provides basic information but lacks depth or has minor inaccuracies. | Significant inaccuracies or lack of detail in presenting the situation and policy. |
| **Review of Arguments & Stances** | Thoroughly analyzes and objectively presents both the owner’s and the employees’ perspectives. Demonstrates understanding of the conflict. | Good analysis of both sides, but misses minor points. | Reviewed arguments but missing points. | Poor or biased presentation of arguments, failing to effectively address both perspectives. |
| **Recommendation** | Provides a well-reasoned, practical, and clear recommendation that addresses the concerns of both parties. Supported by external sources or best practices. | Solid recommendation, but may lack full consideration of both sides or some supporting evidence. | Provides a basic recommendation but lacks supporting evidence. | Vague or ineffective recommendation, lacking justification or feasibility. |
| **Format and APA Style** | Professionally written with strict adherence to APA format, including citations and references. Clear, concise, and well-organized. | Mostly adheres to APA format with minor errors. Well-written and organized. | Satisfactory adherence to APA format, but with several errors or organizational issues. | Poorly written with significant APA format errors and poor organization |

Due 4/21

1. For Week of 4/16 Hacktivism

Assignment Name: Harvesting with a GreeenThumb(DRIVE)

NICE Framework – Legal Advice & Advocacy – Privacy Officer/Privacy Compliance Manager

T0478

GreenThumbDRIVE is a hacktivist group that targets organizations that they deem has committed environmental harm. This included attacking a petroleum company, Hester’s Gases, by infiltrating their internal network, gaining access to and releasing sensitive data. They also defaced their website with their calling card and a coupon for GreenWorks (not the tool company; but their very bad online cookie company). They have also acknowledged their actions in an online statement on a hacking forum they frequent.

Business did suffer for a few weeks while trying to get systems back up. Estimated to have lost about 389,000 in business due to down and repairs.

Your job as the Privacy Officer is to take the details above and identify how the Computer Fraud and Abuse Act (CFAA) applies to this scenario.

*Things to Consider (not to be headers in your papers)*

* *What actions did GreenThumbDRIVE do that violated the law?*
* *What is the severity of the violation? Does the dollar value change anything for the company?*
* *What options does Hester’s Gases have?*

As the Privacy Officer, you are to provide guidance on the law to management and personnel. Your task is to write a report that how the group broke the law, potential legal repercussions and the impact of attack. It is advised that you also share some potential best practices and measures that could be incorporated to prevent similar incidents. The report should be in 2-3 pages in APA format.

Deliverables: **Violation Report in PDF Format**

Rubric:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criteria** | **Excellent (25)** | **Good (15)** | **Satisfactory (10)** | **Needs Improvement (5)** |
| **Information** | Provides highly accurate and detailed information about the CFAA and its application to the actions of GreenThumbDRIVE. | Accurately presents the most relevant information about CFAA, with minor details missing or unclear. | Provides basic information about CFAA but lacks depth or has minor inaccuracies. | Inaccuracies or lack of detail in presenting CFAA and its relevance. |
| **Analysis of the Incident** | Thorough and insightful analysis of how GreenThumbDRIVE's actions violate the CFAA, including consideration of the severity of the violation and its impact on Hester’s Gases. | Good analysis of the violation with some insightful points, but may lack depth in assessing the severity or impact. | Decent analysis, but somewhat surface-level or lacking in detailed consideration of the violation's severity or impact. | Poor or superficial analysis of the incident, failing to effectively link actions to CFAA violations or assess impact. |
| **Recommendation** | Provides well-reasoned, practical, and clear recommendations for best practices and measures to prevent similar incidents. Supported by research or best practices. | Solid recommendations, but may lack full consideration of the incident specifics or depth in supporting evidence. | Basic recommendations are provided but lacks supporting evidence. | Vague or ineffective recommendations, lacking practical applicability or justification. |
| **Format and APA Style** | Professionally written with strict adherence to APA format, including citations and references. Clear, concise, and well-organized. | Mostly adheres to APA format with minor errors. Well-written and organized. | Satisfactory adherence to APA format, but with several errors or organizational issues. | Poorly written with significant APA format errors and poor organization. |

Due: 4/28