Homework #4:

Q1. Once again, let us look at the electric power companies. Use web resources to find an information security (or cybersecurity) policy of a utility company and list some of its key features in the context of what you have learned in this module. Make sure to provide a complete citation of the source. Your answer should not exceed a page.

- Data Classification and Protection: Dominion Energy has developed a sensitive data categorization system that categorizes based upon the level of confidentiality the information requires and applies the appropriate security measures.
- Incident response plan: A thorough and structured process for identifying, responding to, and cybersecurity incident recovery with assigned responsibilities and roles for managing the incident.
- Third Party Vendor Management: To ensure that these third party vendors comply with the security standards of Dominion Energy the continuously check and supervise them due to theses third party vendors having access to these critical systems.
- *Privacy: Dominion energy*. Privacy | Dominion Energy. (n.d.). https://www.dominionenergy.com/privacy

Q2. Look into the security rule of HIPAA and summarize the technical safeguards that it recommends (or enforces) as part of security standards. Once again, use web resources and make sure to provide a complete citation with URL. Your answer should be limited to one page.

- Audit Controls: Utilize software, hardware, or procedures to monitor and record information systems activities that use or hold health info that is protected by electronics.
- Transmission security: Utilize technical security measures to prevent unauthorized access of health info that is protected electronically during transmission over an electronic communications network.
- Access Controls: To ensure that only the software or individuals that have obtained authorization access the electronically protected health information technical procedures and policies are implemented.
- Integrity Controls: Develop policies and procedures to safeguard the health info that is electronically protected from unauthorized alterations or damage.
- (OCR), O. for C. R. (2022, October 20). *Summary of the HIPAA security rule*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
- READ, 5 MIN. (n.d.). *Hipaa Security Rule & Risk Analysis*. American Medical Association. https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis#:~:text=The%20HIPAA%20Security%20Rule%20requires,and%20security%20of%20this%20information

Q3. All educational institutions have to comply with FERPA. Use web resources to write a brief summary of the security implications of FERPA from the institution's perspective. Make sure to provide a complete citation with URL. Your answer should be limited to one page.

- A requirement for FERPA is to safeguard the privacy of student records. Educational Institutions are required to ensure student data is protected from unauthorized access. They may carry this out by utilizing tools such as strict access control and encryption. To comply with FERPA these institutions must also carry out routine monitoring, risk assessments, and faculty and staff training on data security. If these institutions fail to comply with FERPA it may lead to them possibly losing federal funding or legal consequences.
- *Right to privacy (FERPA) – student records*. Virginia Western Community College. (2024, July 24). https://www.virginiawestern.edu/get-started/records/right-to-privacy/