Plan & Scope: The encryption policy for USM CU will comprehensively address the best encryption technology to be employed and the training of staff to effectively support customers and protect data, information processes, and confidential resources. The policy will cover the protection of data at rest, in transit, and in use, both within USM CU's communities and when accessed by staff, customers, or third parties. Encryption tools such as elliptic curve cryptography and BitLocker could be considered for software and application security. Moreover, the policy will ensure compliance with federal and state laws to maintain the confidentiality of employee and customer records and prevent privacy breaches (Garon 2020, p. 108). The Fair Credit Reporting Act will be considered to discourage activities that promote the abuse and exploitation of consumer credit information (Garon 2020, p. 13), and compliance with the Gramm-Leach-Bliley Act will be ensured by providing customers with annual privacy notices and the option to opt out of the sale of their information to third parties (Garon 2020, pp. 116-117). Encryption is a crucial security measure that establishes guidelines for USM CU to protect data from unauthorized access, system vulnerabilities, and theft. The encryption policy will align with federal and state government provisions on data privacy and encryption, promoting the organization's commitment to asset security and meeting industry best practices.

Legal and Moral Obligations: USM CU's legal obligation is to ensure compliance with relevant laws and best practices when handling customer data. Encryption is crucial in safeguarding privacy and limiting unauthorized information sharing (Garon 2020, p. 113). The Fair Credit Reporting Act regulates the disclosure of credit and financial information by credit bureaus, extending these restrictions to financial institutions and prohibiting the sharing of credit information without customer consent (Spinello 2022, p. 179). Morally, USM CU has an obligation to implement robust cybersecurity measures, including encryption, to protect customer assets and maintain a high level of security. This promotes trust, information integrity, and reliability (Spinello 2022, p. 220). The similarities between legal and moral obligations involve the establishment of a secure architecture that protects customer assets and prevents privacy breaches, fostering customer trust in transactions. However, legal obligations are mandatory standards that must be implemented to avoid penalties, while moral obligations reflect the company's commitment to providing a trustworthy and secure environment for customers.

NIST PROTECT function: In addition to its focus on privacy protection for individuals and institutions like USM CU, the National Institute of Standards and Technology (NIST) explores the consequences of privacy on growth prospects (NIST 2020). The NIST PROTECT function aligns with USM CU's encryption policy, which emphasizes the use of encryption technology to promote best practices for data encryption and protect customer privacy. NIST supports the rigorous obligations placed on institutions to secure collected data and restricts the sale and use of data (Garon 2020). They recognize the benefits of such practices in managing risks to individual privacy. The NIST PROTECT framework highlights the importance of privacy and explores risk mitigation strategies for enterprises to stay current with technology trends, reinforcing privacy risk management.

References

Bardach, E. (2024). A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving. CQ Press.

Garon, J. M. (2020). Garon's A Short & Happy Guide to Privacy and Cybersecurity Law. West Academic Publishing. https://ecampus.vitalsource.com/books/9781647084691

Spinello, R. A. (2021). Cyber-ethics: Morality and law in cyberspace (7th ed.). Jones & Bartlett Learning