OLD DOMINION UNIVERSITY

CYSE 300: INTRODUCTION TO CYBERSECURITY

Information Security Properties

George “Trey” Smith

01249099

Information security policy is well known to follow strict rules and guidelines to help others keep their digital information safe. We, as policymakers, have to ensure that the CIA triad is well defined in our policy and standards. Seeing that we have to ensure the protection of our data, our policy must be able to address major threats and enforce operations to mitigate these risks.

Access control and authentication is one of the major security concerns that we need to focus on. Corporate information systems are one of the most important things to cover when making policy. According to the NIST framework, our policy should have strong authentication methods such as multi-factor authentication (MFA) and regular password updates with strict regulations (Grassi et al., 2017). Regulations such as not having similar words in passwords or having too many plain words together could make this policy strong.

Next, we have data protection and encryption. Due to our servers containing high-value information, our policy should have end-to-end encryption set up for it. Our policy should also give a standard for "data masking and tokenization." It can protect sensitive information from internal threats and leaks (IBM, United *States*, 2025).

After that, we have network security and segmentation. Our policy should have segmented networks so we can reduce attack surfaces that can be targeted within a breach. Our security should also have multiple intrusion detection systems, intrusion prevention systems, and firewalls. Having these in place will help detect and prevent any breaches that can occur so that we can take the appropriate measures to counter and/or assess. We should also introduce a zero-trust system so that constant verification can lock out any bad actors within the system (Grassi et al., 2017).

After this, we should focus on monitoring and incident response. Being able to detect and respond to any threats within our systems should be a big priority. This policy should have real-time logging and security monitoring so that all logs can be analyzed for forensics. Additionally, we should have a set standard for incident response so every employee knows what to do when these attacks happen (Grassi et al., 2017).

Lastly, a great policy must have periodical security audits and vulnerability assessments. These audits and assessments can help identify any weaknesses in the system that might need to be patched or updated. Having regular pentesting helps ensure that security measures are effective and makes sure that we meet regulatory requirements. These policies keep organizations actively able to identify and stop vulnerabilities.

In conclusion, having multi-layered security systems with a strong policy can help prevent and mitigate attackers from being able to access your system. By assuring that a policy hits all five of these main topics by including what is necessary, it can ensure the maximum amount of security for all data within the organization.

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). Digital identity guidelines: authentication and lifecycle management. *NIST Special Publication 800-63B*, *800-63B*. https://doi.org/10.6028/nist.sp.800-63b

IBM - United States. (2025). Ibm.com. https://www.ibm.com/us-en