**Examples of Maintenance Policies on Cybersecurity (NIST and ISO)**

This paper provides real examples of maintenance policies that are used by companies in regard to cybersecurity, and those that complies with ISO and NIST requirements and controls. The following are the identified maintenance policies.

1. **Data security policy: Employee requirements:** This is an example of policy which provides an outline of behaviors expected of employees when dealing with company’s data. This is also maintenance policy that link employee to Acceptable Use Policy (AUP), security training, and information security policy, and this policy provides guidance to the use on the required behaviors when handling/ managing data (Calder, 2018). In terms of the scope, it is concerned with any employee or individual who have access to company’s systems or data.
2. **Workspace Full Disk Encryption:** This is an example of policy has been recommended by NIST and is intended to act as a guideline for the organizations needing to implement or update/ maintain their full disk encryption control policy. The company can adopt and adapt this policy especially in line with usability requirements or in accordance with the date that need to be protected. This policy helps organizations to ensure restriction of confidentiality and prevention of sensitive data from damage (Syihabuddin et al., 2020). The scope of this maintenance policy is based on company’s workstations, virtual machines. The policy in the organization is to have all devices with full disk encryption enabled.
3. **Data Classification and Handling Policy:** This policy is geared towards minimizing unauthorized sharing of classified information, data maintenance. The company can review this policy by assigning roles, coordinating, and reviewing the implementation of security across the organization. The protection and overall privacy for individual and organizational information is a major concern in the application of this policy (Rittinghouse et al., 2003). This policy provides guidance on how data is maintained, accessed, and protected. Additionally, the policy gives guidance of data classification and level of dissemination that is allowed.
4. **Security Incidence Response Plan-** This is an example of cybersecurity policy plan as provided by NIST and focuses on initiating appropriate remediation actions during incidents. With this policy and security incident strategy, it is paramount in providing guideline which include initial response threats, priorities, identification, and appropriated maintenance security polices for the organization information systems (Calder, 2018).
5. **Intrusion prevention policy:** This is an example of maintenance policy relating to cybersecurity and is stipulated in NIST and ISO 27001 and ISO/ IEC 27039. The policy is meant to detect and automatically block network attacks and browser related attacks (Mesker et al.,2014). Additionally, this cyber security example is used in protecting applications from vulnerabilities by checking the content of more than one data packages and detecting all malwares

References

Calder, A. (2018). *NIST Cybersecurity Framework: A pocket guide*. IT Governance Publishing Ltd.

Mesker, K., Engineer, I. C., & Chevron, E. T. C. (2014, October). Adapting NIST Cybersecurity Framework for Risk Assessment. In *NIST Conference*.

Rittinghouse, J., Hancock, W. M., & CISSP, C. (2003). *Cybersecurity operations handbook*. Digital Press.

Syihabuddin, A., Suryanto, Y., & Salman, M. (2020). Risk Management in Data Centers Using ISO 31000: 2018 Case Study: XYZ Agency. *Science, Technology, Engineering, Economics, Education, and Mathematics*, *1*(1).