**Create an IT Policy Evaluation Tool to Evaluate an IT Policy**

Francis Cobbinah

School of Technology: Northcentral University

TIM7040: Technology Policy and Strategy

Dr. Lyn Lazar

January 10, 2021

Francis,

Though you have some good information in your paper, you needed to create a tool to use in evaluating IT policies. You gave the information, but you needed to put your evaluation criteria into a table or checklist to quickly and easily evaluate policies. In part two of the assignment, you needed to include a chart with your criterion and then use your tool to evaluation the policy. You also needed to discuss how the organization uses IT policy strategically.

Take a look at the highlights and comments and let me know what questions you have.

Dr. Lyn Lazar

Then, create a report in which you summarize the following:

1. Provide a description of the organization that you chose, along with the web address for the IT policy.
2. Describe the IT policy at a high level.
3. Present a chart depicting each criterion with its description and a scale showing the requirements for each level in the scale of the evaluation tool (in an appendix).
4. Create a narrative to explain the rationale for the criteria and rating scale.
5. Use your tool to evaluate the IT policy and provide strengths and weaknesses.
6. Provide three recommendations to improve the IT policy.
7. Explain how this organization uses IT policy strategically.

**Policy Evaluation Tool: Part 1**

**Cyber-Security Awareness Policy**

The policy's objective is to educate users on how to enforce and coordinate a security program across the organization through the disclosure and effective communication of security measures. The policy creates a general approach to information security that all the stakeholders should adopt. Some of the policy elements are utility, integrity, confidentiality, authenticity, and availability. The target audience for the policy is all the employees within the organization. The cyber-security tool developed is provided below.

|  |  |  |
| --- | --- | --- |
| The Cyber-security Policy Tool | | |
| The tool has six effectiveness levels | | |
| Below is a summary of these levels. | | |
| Effectiveness level | Criteria and Definition of the levels | Explanation |
| Level 1 | Documentation and awareness are lacking in the policy | The specific risk areas are not identified and the control measures are missing |
| Level 2 | There is inconsistency in cyber controls | The available cyber control measures cannot mitigate the potential risks |
| Level 3 | Standardized practice is in place though partially effective | Cyber-security control measures are put in place though formal approval and definition are unavailable |
| Level 4 | Cyber-security control measures are well-defined, approved, and implemented. There is demonstration of implementation. | There are well-established cyber-security procedures, standards, and policies. The procedures, standards and policies comply with the security documentation. The key performance indicators are provided. |
| Level 5 | There is periodic assessment of cyber control measures. | Key trends and risk indicators are provided to determine the cyber-security controls’ effectiveness. |
| Level 6 | Cyber control measures are effective and can be replicated in a continuous improvement plan. | The organizational cyber-security plan emphasizes improvement, effectiveness, and compliance of cyber-security control measures. |

The stakeholders who should observe the policy are individuals interested in the organization. They can either be internal or external stakeholders. Organizational management is responsible for the evaluation and approval of the policy. The policy should be communicated to all the stakeholders through scheduled training sessions. The policy can be revised at any time when the need arises. The contents considered when developing the policy evaluation tool are discussed below.

**Policy Contents**

|  |  |
| --- | --- |
| Confidentiality: | Unauthorized persons should not have access to data. |
| Availability: | Users should have access to the information that they need at any time. |
| Integrity: | The data in the IT systems should be complete, accurate, and intact (Alsmadi, 2019). |
| Hierarchical authority: | The organization’s senior manager can decide who should access or share data and when this should be done (Al-Shomrani et al., 2017) |
| Network standards and guidelines: | Users can only access the company’s servers and networks through unique logins that must require authentication such as tokens, Identity Cards, biometric authentication, or passwords (Ajayi, 2016). |
| Data Classification: | Data needs to be classified as either public, confidential, secretive, or highly secretive (Carr, 2016). |
| Data operations: | Data storage systems should have anti-malware protection, a firewall, and encryption at the lowest security level (Moallem, 2019). |
| Data backup: | There should be a secure cloud storage. |
| Data transfer: | Data transfer should only be done through secure protocols. After transmitting information through a public network or copying such information to portable devices, encryption is inevitable. |
| Social engineering protective measures: | All employees are responsible for reporting and preventing phishing emails. All computers and laptops require secure cable locks. Printer areas need to be clean to ensure that information does not fall into wrong hands. |
| Employees’ rights, responsibilities, and duties: | The human resource manager needs to carry out periodic updates and reviews of change management, education, and incident management. According to Lomas (2020), it is the role of the human resource manager to enhance the effectiveness of the implementation of cyber-security policies. |

A cyber-security framework needs to adhere to the following framework.

**The Cyber-security Framework Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Identification | protection | Detection | response | recovery |
| Asset management | Provide access control and identity management | Detect risky events and anomalies | Plan for effective response | Develop an actionable recovery plan |
| Organizational environment | Provide training and awareness | Ensure continuous security monitoring | Address communications issues | Prioritize improvements |
| Risk management strategy | Emphasize maintenance | Detect risky events. | Provide immediate response actions | Emphasize improvements |
| Risk assessment | Identify relevant procedures and processes | Develop information protection measures | Provide mitigation measures | Create room for improvements |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Cyber-security Framework’s Checklist | | | | | |
| Governance | | | compliance and risk management | | |
| Leadership | Risk management | Legal Compliance | Industrial standards compliance | continuous review | Auditing |
|  | Technology and operations | | | | Involvement of third-parties |
| Policy Implementation Strategy | asset management | physical security | human resources | | Apply contract |
| Responsibilities and roles | Manage change | Secure applications | manage access and identity | Develop a comprehensive cyber-security architecture | Manage vendors |
| Training | Managing vulnerabilities | Managing threats | Managing cyber-security incidents | | Emphasize cloud computing |

From the above framework, a practical cyber-security framework is the one that addresses issues relating to governance, leadership, policy implementation strategies, responsibilities and roles, and training. The key stakeholders in an organization need to be trained about managing threats, vulnerabilities, and cyber-security incidents. The organization needs to manage change effectively, secure applications, develop a comprehensive cyber-security architecture and manage access and identity. The organization’s policy implementation strategy should address human resource, physical security, and asset management issues. These are the issues that are related to technology and operations.

**Part Two**

The University of North Alabama has a well-developed 'cyber-security awareness training program'. The purpose of [the program](https://www.una.edu/humanresources/files/forms-links/Security%20Awareness%20Training%20Program%20Requirements%20and%20FAQs%20for%20the%20Web.pdf) is to protect the University's intellectual property and confidential or personal information. The University's policy document provides standards and guidelines that all the employees should follow. Everyone who receives information or service through the University's information systems has to follow these standards.

The policy applies to the use of all the University's resources, including computers, networking infrastructure and devices, and software. The aspects covered in the policy include proper antivirus protection, data backup, proper password usage, and violations of security policy. The University requires all the staff members to attend annual online training.

In the University's [acceptable use statement](https://www.una.edu/its/una-it-policy.html), all employees and students or any other individual who might be interested in using the University's resources need to abide by the following guidelines. The effectiveness of these guidelines is evaluated based on the IT policy evaluation tool provided earlier. When using the University's information technologies, everyone needs to use them in a way that supports a conducive academic climate. These technologies refer to communication networks, data, software, and, hardware. The University's information systems include; mobile devices, personal computers, single-user terminals and other multi-user terminals connected to networks or free-standing.

 The University allows its staff to access networks, software, and hardware if the intended purpose is to enhance the academic experience. That is one of the qualities of an effective IT policy. Authorization is required to ensure that technologies are used as necessary. According to UNA policy documents, users can only use accounts in the University's computing systems, but they don't own the accounts. Such a measure is necessary to address vandalism, theft, and misuse of the University's resources.

The University's unacceptable use guidelines are clearly stated in the policy document. No one can use access network or computing technologies if they misuse information, network, or computing devices. Users are accountable for their actions, and they can be prosecuted if they act inappropriately. The policy is designed in a way that would enhance the achievement of organizational goals. It does not hinder the stakeholders' initiative since it has a narrow outline that does not require a complex interpretation process. Besides, the policy document is not mutually contradictory, and all the guidelines are consistent. Therefore, there cannot be any delay or confusion during the implementation process.

The guidelines provided in the policy document are also flexible, logical, and sound. The policy is a reflection of both the external and internal organizational environment. The language used can be clearly understood. Besides, everyone who is affected by the policy has been defined. The University use its IT policy strategically to protect intellectual property. It also protects its information systems from damage and theft.

Although the policy is effective, the University needs to apply the following recommendations. Firstly, the University's policy document needs to include the anti-exploit, anti-malware, firewall, and antivirus software that should be used to protect technologies. Secondly, there should be standards that should be followed in case of a threat or an incident. Thirdly, the management should provide information to show that the policy conforms to regulatory requirements.

References

Ajayi, E. F. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*(1), 1-12. doi:10.5897/jiis2015.0089

Al-Shomrani, A., Fathy, F., & Jambi, K. (2017). Policy enforcement for big data security. *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*. doi:10.1109/anti-cybercrime.2017.7905266

Alsmadi, I. (2019). Cyber policy and strategy management. *The NICE Cyber Security Framework*, 181-203. Doi: 10.1007/978-3-030-02360-7\_8

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62. doi:10.1111/1468-2346.12504

Lomas, E. (2020). Information governance and cyber security: Framework for securing and managing information effectively and ethically. *Cyber security for Information Professionals*, 109-130. Doi: 10.1201/9781003042235-6

Moallem, A. (2019). Student’s cyber security awareness. *Cyber security Awareness among Students and Faculty*, 7-15. Doi: 10.1201/9780429031908-2