Assignment 7
Cybersecurity Policy Analysis

CYBR 3080 IT Service Delivery Security

Gregory Stephens

Security of Personally Owned Devices That Access or Maintain 601.33 Sensitive Institutional Data for Michigan University

What Was Done Well

- The policy makes its goal obvious: to protect sensitive institutional information accessed or maintained on personally owned devices (PODs). This emphasis makes the extent and purpose of the policy clear to stakeholders.[1]
- Comprehensive coverage: It covers essential elements including access controls, incident reporting procedures, encryption standards, and device security criteria. These components follow established guidelines for sensitive data security.[2]
- The policy ensures conformity with external standards by referencing compliance with relevant regulations and rules.[3]

Areas for Improvement

- Training and Awareness: The policy assumes that users will know how to implement its requirements (e.g., enabling encryption). Including mentions of workshops or learning tools would improve usability.[2]
- Language access: Though the document is thorough, some parts could be hard for non-technical readers to grasp. Including a glossary and simplifying technical language could help you understand.[1]
- Although the policy sets out penalties for not following it, it does not expressly state how offenses will be found or enforced. Including information on audits or monitoring solutions would help to improve accountability.[3]

Type of Policy

This policy is a Security Policy designed to protect sensitive institutional data by establishing guidelines for the use of personally owned devices (PODs).

- User accountability: the policy sets up a governance system of security policies by defining repercussions for non-compliance and delegating end-user obligations.
- Regarding technical controls, it lists technology requirements—including encryption, password demands, and the ability for remote wipe—that are characteristic of security-focused policies.
- The policy stresses lowering the hazards linked with PODs access or storing of sensitive information. This is in line with the main aim of security regulations to protect assets from dangers.

NIST Classification: Issue-Specific Policy:

- Conformity with SPG 601.33: This policy is expressly designed to address the dangers of accessing or maintaining sensitive institutional data with personally owned devices (PODs). It sets out demands—including encryption, password management, and incident reporting—that are all custom-designed to reduce the special threats of pods.[2;4]

CISSP Classification: Regulatory Policy:

- The policy specifically mentions conformity with statutes and regulations including FERPA (Family Educational Rights and Privacy Act) hence Alignment with SPG 601.33: It also states repercussions for non-compliance, therefore users working with sensitive institutional information must follow it.[3;4]

Challenges and Proposed Solutions

Challenge One:
One major challenge is seeing that the policy is understood and followed by all types of consumers—from professors and staff to students and subcontractors. Non-technical customers could find it difficult to meet encryption or remote wipe guidelines.[1]

Solution:

- Host practical seminars for staff and faculty.
- Develop videos about common student problems and FAQs.
- Provide IT help from one point to help people set their gadgets in line with rules.
- Reminders and knowledge campaigns should be put in regularly to support adherence.

Challenge Two:
Monitoring and Enforcing Compliance. There are no obvious procedures in the policy for discovering infractions or guaranteeing continuous compliance. Users can forget security precautions and raise data breach threats without being closely monitored.[2]

Solution:

- Use automated solutions to track compliance, including software agents on registered PODs that check encryption status and password strength.
- Regularly review high-risk areas or divisions of tools used to access sensitive information.
- Create a non-compliance response plan with warnings to deny access privileges.

References

1) https://spg.umich.edu/sites/default/files/policies/601x33%20Security%20of%20Personally%20Owned%20Devices%20That%20Access%20or%20Maintain%20Sensitive%20Institutional%20Data.pdf
2) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
3) https://destcert.com/resources/domain-1-security-and-risk-management/
4) https://chat.qwen.ai/