POLICIES PROJECT

Project for Coursera Course

Juan Felipe **Rodríguez Galindo**

EVALUATION

The objective of this task is to help you understand that not all organizational policies are the same. You will write your own security policy for a midsize business based on other organizational policies that have been written in the industry.

REVIEW CRITERIA

Homework will be graded according to the **strictness of the policy and supporting research** conducted.

BACKGROUND AND INSTRUCTIONS

BACKGROUND:

In Lesson 2, we discussed the need for organizational policies. Most organizational policies are different in some way, but they can contain many of the same characteristics. Policies are meant to be followed and generally don't contain a lot of unnecessary information or rules to follow. The information in the policy usually comes from something that happened in the past.

In this task, you will need to conduct research on what organizational policies look like, discuss how they are the same or different. Then you will choose one of your own to write based on something you know.

For example, I love to play video games, so I will search the website of some video game retailers and see their policies. Then I will compare and discuss them.

Then I'll take the same concept, my video game retailer, and design my own policy based on one of the example policies in the examples section of Lesson 2 written by SANS.

STEPS:

- Lesson 2 Review
- Choose 3-4 companies or organizations to review your policies.
- Discuss how the policies differ from each other and discuss how they are alike.
- Also, provide your own perspective on how the policies might affect you as a consumer.
- Pick a sample SANS policy and create your own for the industry or organization that interests you.
- Reflect on the experience and how you approached the problem.

YOUR MISSION:

Submit your responses in the text boxes below.

- **Choose 3-4 companies** or organizations to review their policies. How**are they different and how could they be the same**? Submit the **names of the companies** and **policies you reviewed**.
- Pick a **sample SANS policy** and **create your own** for the industry or organization that interests you.
- **Reflect on the experience** and **how you approached the problem**.

DEVELOPMENT PROJECT

1. **Revised policies:** Policies for the creation of passwords.

   Companies Reviewed: Microsoft, IBM, Weill cornell medicine, University of Georgia, University of Seville.

   Differences and Similarities: In the first place the **Differences** which lie mainly in the extension of the policies and the field that each one of them covers, that is, for example in the policies that Windows 10 handles, which are basically the same as Outlook, we see that there is no relevance to how the company handles the security of user-given passwords. Another big difference is the fact that some companies close the step of exporting passwords outside the organization, those are the ones that I emphasize the most or that have a greater influence for the course since they have a very high weight in what is developed in the course.

   Now to state some **similarities that are** also very important, we can see that each company uses a series of guidelines in an integrated way to improve the security of passwords, for example the length, the number of numbers that it must contain, among others.

   To make the comparison, although I review various sources, I took as main policies for the exercise those of the **University of Seville**, the **University of Georgia** and the company **Weill Cornell Medicine Information Technologies & Services**, since for me they were the ones that stand out the most within the field of political, since they had many differences and very different points of view from each other.

   As for these, we can denote the **similarities** that the three do not allow the output of passwords outside the institution and that all of these are not transferable even within organizations, another similar characteristic is that they have a guide for construction with in order to be safe in the institution.

   Now talking about the **differences** we can talk about the University of Georgia which establishes a section of different or complementary policies for the administrators and developers of the system, on the other hand the most notable difference occurs in the policies of Weill Cornell Medicine since they are the most robust of these three since it has several sections in order to cover all possible situations that may arise, for example when the account is blocked, the responsibilities that the system must have, the user's responsibilities with the password, among others.

2. Guidelines for the construction of passwords applied to medium-sized companies in Colombia.

Summary. Passwords are a critical component of information security. Passwords are used to protect user accounts; however, a poorly constructed password can result in compromise of individual systems, data, or networks. This guide provides the best practices for creating secure passwords, applied to the small and medium-sized business sector within the Colombian productive sector.

Purpose. The main purpose of these guidelines is to provide a guide to improve current practices for the creation of strong passwords, within small and medium-sized companies in Colombia.

Scope. This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guide applies to all passwords, including but not limited to user-level accounts, system-level accounts, web accounts, email accounts, screen saver protection, voicemail, and router logins local.

Goals. Establish policies or good practices in the use of a password management system for access control.

Statement of guidelines. The main points of the policy that arises are:

- Password management. Password management in the world of information technology is one of the most delicate aspects to ensure access to your systems. In short, it deals with:
    - Identifying the equipment, services and applications that need to be accessed.
    - Define how the default keys are generated, as well as their format.
    - Distribution of the generated keys (Define method and encryption, how the keys are activated).
    - Key storage, secure repositories and backup copies.
    - Clearly determine how and who has access in order to perform a proper system audit.
    - Establish periods in which passwords are secure in order to make the security of a cyclical process and that it changes continuously in order to reinforce security.
    - Determine the access revocation processes by the system when a user is discharged from the organization
    - Passwords must be strong, to create a secure password we will follow a series of guidelines to be able to make the correct strength of the password which will be at end of this section.

- External authentication techniques, in the case of a small company it is not necessary to use this methodology to make the entry, although there may always be the possibility of it being handled, for which we will also cover the possibility of implementation.
    - At this point, after carefully reviewing the different techniques that can be used, it is evident that for small or medium-sized companies, the best form of authentication if it is required to use these forms will be social-login, which with alternatives such as google and microsoft that they have very secure servers to perform a reliable authentication process.
- You should not use the passwords generated by the system, for this we must make an immediate change in the first login in the system.
- Password change periodically, in order to make the use of penetration techniques more difficult to the system in which we are.
- Take into account the use of a password generator since if you use a very simple one it can be very easy to crack.
- Creation of metadata for password generation to save the reason for creating a key, the date, and other vital data from which information can be extracted in the event of an audit by the system administrator.
- Try not to use the same password outside the company or with other services in order not to spread the vulnerabilities of the password to another system.
- Use of double factor authentication to enter the system (either to another secure email or with a biometric key).
- Do not share the password or with anyone outside the company (or put them physically in papers or notebooks that are at the mercy of other people in the organization)
- It is vital not to use the tool that some devices or browsers have to remember passwords as these can be a major vulnerability if the device leaves the company.

Checklist or policy compliance. Checklist in order to verify that the guidelines are met.

Related standards, policies and processes.
policy Passwordof the University of Seville.

References.
https://blog.devolutions.net/2018/02/top-10-password-policies-and-best-practices-for-system-administrators

APPENDIX
In order for the password to be robust, it is recommended that the passwords
- must be composed of at least eight characters;
- This must combine characters of different types (lower case, upper case, symbols and numbers);

- Passwords should not contain the following types of words:
    - single words in any language (words from dictionaries are not recommended);
    - proper names, dates, places or personal data;
    - words that are made up of nearby characters on the keyboard (eg 123456);
    - excessively short words.
- The use of keys made up of elements or words that can be public or very simple to guess (eg name + date of birth) will be avoided;
- Stronger passwords will be established for access to those most critical services or applications, carrying applications with two-factor authentication;
- The foregoing will be taken into account also in the case of using passphrase type passwords (long password made up of a sequence of words)

3. **Experience ->**

   The creation of these policies in my opinion are quite complex and require a great deal of hard work in the initial process of development, although we have tools such as those provided by SANS, a large part of this process must also be accommodated or customized according to the needs of the company in which we work. Also, for each use case, specific policies could also be created that grant a systems administrator a more viable option to audit or manage a system, this seeking the most optimal efficiency and processes.

   Also for the creation or stipulation of these, it is also preferable to take as a basis a spiral development methodology for the management and constant improvement of these policies, this process can be compared as that of making certain updates to our policies constantly and iterative.

   How you approached the problem->

   In the first place the choice of a policy, the choice of a policy for me was a fundamental section during the development of a work carried out comfortably and preserving a high quality. For this reason, I chose the use and creation of passwords within a system as the main axis, since the issue is usually ignored by people who interact with systems using weak keys.

   Secondly, the choice of the sources from which we will collect information to develop our own policies, also a fundamental step since as soon as we can follow or review an already proven and well-documented model, we can carry out the process of stipulating rules by time to choose or generate a password.

   Now to complete a complete review, that is, personally evaluate the model and then compare it with other policy models used within the information technology industry, in order to detect possible flaws and add some robustness to the policies generated.

REFERENCES

- https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
- https://www.ibm.com/support/knowledgecenter/en/ssw_aix_72/__security__/aix_sec_expert_pwd_policy_settings.html
- https://its.weill.cornell.edu/policies/1115-password-policy-and-guidelines
- https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/passwords/password_standard/
- https://blog.devolutions.net/2018/02/top-10-password-policies-and-best-practices-for-system-administrators
- https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blta5be14c7136a535f /5e9dde89db124263e8afce3d/password_construction_guidelines.pdf
- https://sic.us.es/sites/default/files/seguridad/politica_de_contrasennas_us.pdf
- https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas .pdf
- https://docs.microsoft.com/en-us/azure/active-directory/develop/
- Echeverry, AML, & Sánchez, PAV (2016). Password management policy for end users. *Scientia et technica*, *21*(2), 128-134.