

Security Policies and Workstation Standardization

Cybersecurity is stronger when it is planned and based on best practices and frameworks that are engineered to protect each company from both external and internal threats.

The plan we designed is also based on these international best practices and frameworks, in particular NIST (The National Institute of Standards and Technology), IAM Framework and AAA methodology.

Security policies are a group of security settings that enhance the protection by helping to manage several aspects of security within a company. From passwords to external drives, lockout periods or RDP connections.

We defined a set of security policies, security recommendations and possible upgrades in the future as the company grows. These can be reviewed, or changed, according to both the needs and the plans of the company.

In regard with the workstation standardization besides the Wallpaper we defined a set of rules to enforce a more uniform workstation not only aesthetically but also in security and overall settings. You can skip to Objectives and Policies if you want to go directly to these settings and how they work.

A step by step guide and manual regarding these policies and documentation about both frameworks will be provided on the github.

Categories and levels of recommendation

With this approach we set a level of categories and recommendations for policies that the company should consider, while providing the best solution for this project. In this document we find the list of policies we consider for this stage. Policies applied to meet the project objective were left outside of recommendation levels as they are not considered recommendations.

Three levels of recommendation:

A) Critical: These policies should be applied now to either enhance already applied policies or to enforce a more secure environment.

B) Needed: These policies should be considered as a need for the company. Although not critical, the absence of these policies mean a less secure system.

C) Recommended: These policies are recommended to help improve the security and overall performance of the company. Aesthetics and other similar policies will be considered here.

- - NIST

The National Institute of Standards and Technology is part of the U.S. Department of Commerce, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations. The NIST is also responsible for frameworks such as NIST CSF 2.0, develops cybersecurity and privacy standards, guidelines, best practices, and resources to meet the needs of U.S. industry, federal agencies, and the broader public.

- - What is the IAM Framework?

Identity and Access Management (IAM) is a framework that focuses on Identity management and access management, a group of security controls that manage who has access to the resources of a company. Different roles have different permissions and privileges.

IAM identifies users by verifying their information, authenticates the profile via password or other security measurements and authorizes that user to a set of specific resources. Part of the IAM Framework involves AAA methodology that was important to determine the structure of both policies applied and recommendations. Also, it's important because it establishes who has access to specific resources while keeping track of activity.

The AAA methodology involves three stages:

- **Authentication:** The process of verifying who the user claims to be. Traditionally this is done using a password or other form of confirmation. Nowadays, this is usually not enough to have a secure environment, so other policies or rules should be applied to enforce security.

- **Authorization:** The process of verifying what resources a user can actually access with their profile. Authorization dictates what resources a user can have available, the least privileged principle can be seen here, the IT manager has access to more resources than other IT employees.

- **Accounting:** Keeps track of user activity while users are logged on a network. It helps monitor, analyze trends, and audit user activity.

Both IAM and AAA helps an organization's IT department strike the right balance between keeping important data and resources inaccessible to most but still accessible to some. IAM makes it possible to set controls that grant secure access to employees and devices while making it difficult or impossible for outsiders to get through.

-- Objectives and Policies

The objective is to implement strong and cohesive security policies for the company based on the above frameworks. We also had in consideration the least privileged principle, i.e the concept that each worker will only have the specific tools and permissions to fulfil his job.

These security policies are based on 3 levels: Critical, Needed, Recommended. These levels of recommendation are designed by us according to the size of the company, as the company grows some of these policies must be changed or upgraded. Below the policies requested for this project and recommendations.

Password Policy: Users will have to set a password on first log in, users will have a 30 day period for each password, different from the previous 8 passwords (when applied) and use special characters to enhance security.

- 1) Enforce password history: last 8 passwords
- 2) Maximum password age: 30 days
- 3) Minimum password age: 29 days
- 4) Minimum password length: 10 characters
- 5) Password must meet complexity requirement

Wallpaper: All SecureEdge Inc. employees share the same wallpaper.

Taskbar: All taskbar settings are locked, users can't resize, move or rearrange the taskbar, they also lose access to the taskbar control panel, this way all employees share the same taskbar and wallpaper. We also disabled all balloon notifications and future advertisement balloon notifications.

CRITICAL:

Lockout Period: Lockout Period forces users to wait in case of wrong password combinations. This enhances security and mitigates possible brute force and dictionary attacks.

- 1) Account lockout duration: 20 minutes
- 2) Account lockout threshold: 5 invalid logon attempts
- 3) Allow administrator account lockout: Enable
- 4) Reset account lockout counter after: 15 minutes

Change System Time: Only the IT manager can change the System Time. This can prevent several issues such as computers that belong to a domain not be able to authenticate themselves, time stamps on event log entries could be made inaccurate, time stamps on files and folders that are created or modified could be incorrect or other critical issues.

Disabled Windows Installer: All users and employees will only not be able to install any software via Windows Installer. Only applications previously approved by the IT team. Executables and Scripts can still be runned. As the company grows this policy should be upgraded to AppLocker with a more granular approach and more secure preventing not only Windows Installer but also Executables, scripts and other files.

NEEDED:

Deny all removable storage access: Block USB Drives and other storage access units like SD cards or external discs. This can prevent not only but also malware from being installed.

Prohibit access to the control panel: Only the IT team should have access to the control panel. This will prevent any unwanted system settings to be changed.

Prohibit access to the command prompt: Only the IT team should have access to the command prompt. This will prevent any unwanted commands or scripts to be executed

Lock Screen: This will lock screen after a certain time of inactivity, we advise 5min max. Highly needed or Critical if the employee works in any work space with other people.

RECOMMENDED:

BitLocker: Bitlocker protects data by encrypting drives, this is Needed or Critical as the company grows. Recommended if the company already deals with confidential or any other type of high risk information.

Block unauthorized browser extensions: Block any extensions to prevent malicious extensions or any data from being compromised. Browser settings can also be applied to enhance protection.

Force hibernation after extended inactivity: Force hibernation after a determined period of inactivity, we would recommend 10 to 15min, Highly needed or Critical if the employee works in any work space with other people.

