**Security policy for an organization**

It is an organization's document that defines how the organization can be protected from threats and how to deal with them when they occur. These policies should be updated regularly to keep pace with the problems that the company will face in the future

* 1. **1. Data backup**

1. Making a copy of the data to save into a secondary location it in case of losing the original data, deletion, or disaster, which is then restored. It is also a key component of the Disaster Recovery Plan and Business Continuity Strategy
2. Scope: The important company information must be backed up, including database, user information, and logs
3. **- List at least 5 policies to save this data.**
4. Sort data by type and need.
5. Sort data by lifecycle.
6. Choose what to delete and when to delete it.
7. Choose the types of backups and their frequency.
8. Select a cost-effective and compliant data backup service.

**2. Clean desk policy:**

It is a method that determines how employees can leave their offices when leaving by getting rid of all existing papers in order to prevent unauthorized access to data

Scope: all Organization employees

Polices:

1. **- List at least 5 policies.**
2. Employees are not to leave sensitive data exposed in places where it could be viewed by anyone outside the organization.
3. When employees are not at their desks, any printed materials containing sensitive information should be maintained in a locked area.
4. All employees are responsible for securely destroying any printed items containing sensitive information before disposal.
5. When working in a public place (such as a coffee shop or in an airport), employees should use a privacy screen.
6. All devices (including laptops and phones) must be set to auto-lock with a maximum timeout of 15 minutes when it is unused.
7. **3. Remote access policy:**

There are employees who are remote work, this requires us to explain to them how they can safely connect to the company’s network through the remote access policy document. A virtual private network (VPN) Helps transmit information over the network safely, so we have to put a policy for it because of the misconfiguration.

Scope: Remote-work employees

Policies:

**- List at least 2 policies.**

1. Authorized users are not permitted to connect to the company’s VPN when the host is connected to a network other than the user's personal home network or a trusted third-party network. Users must not connect to the company’s VPN while also connecting to another VPN.
2. Users must take caution when connecting to networks in public places such as airports, coffee shops, and so on, and must not connect to the Company's internal network (even via VPN) if they are on an insecure, public network.

**4. Passwords:**

Passwords are an important component of security. A weak password leads to unauthorized access to the data and then it is tampered with, so it is necessary to put controls in order not to be weak.

Goal: is to protect accounts in strong passwords that are difficult to know

Scope: All Organization employees, third parties and customers

Police:

1. **- List at least 7 policies.**
2. 10-day validity
3. A minimum of 10 characters is required.
4. A maximum of 20 characters is permitted.
5. At least two special characters are required.
6. During the initial log in, the user must change the default password.
7. Number of passwords to remember
8. Prohibit password sharing.
9. **5. physical access control:**

To access comprehensive security, individuals must be authenticated based on the things and data they are allowed to see.

Policies:

1. **- List at least 4 policies.**
2. No access cards or keys may be shared or loaned to others.
3. No longer required access cards and/or keys must be returned to the Department of Public Safety.
4. Cards shall not be transferred to another person without going through the return process.
5. Access cards and/or keys that have been lost or stolen must be reported to the Department of Public Safety.
6. Depending on the criticality of the resources being safeguarded, card access records and key logs for IT facilities must be retained for routine inspection.

**6. Firewall and VPN policy:**

The firewall is one of the most important elements of network security because it monitors traffic and intercepts it if it is a threat. The VPN is also important to hide IP address of devices over the internet and provide a secure encryption for the data.

Policies:

1. **- List at least 3 policies.**
2. The firewall should be placed in a restricted access area where access is granted only as needed.
3. Only the Firewall Administrator should have logical access to the firewall (s).
4. Patches advised by the firewall vendor should be installed as soon as possible, with management's consent.

**7. Third party policy:**

In order to preserve our data that is shared with third parties through the VPN, we must set limits so that they do not exceed them and access unauthorized data for them.

From these police is not to see the personal information of customers.

Policies:

1. **- List at least 3 policies to save this data.**
2. Third parties should be provided access to elements of the business that they may require.
3. Constantly monitor how third parties use your data.
4. If a third-party connection is considered as a security risk, the IT Manager will have the right to disable it.

**- Evaluate the tools in the policy.**

1. Use a firewall or an Access Control List (ACL) to protect the company's network from the network of the third party.
2. To secure internal network resources, systems requiring third-party access should be placed in a demilitarized zone (DMZ).