**Security Policy**

* **Architecture**

The architecture must separate the web server and DNS server from the other internal servers like database server and FTP Server. So to do that, the web server and DNS server can be group up in a demilitarized zone (DMZ) which the web server, and the DNS server that will allow the public to access only.

Then, between the DMZ and the internal network, firewall must be setup to restrict the unauthorized user to be able to access the internal server like the database server and the FTP server.

* **Data Security**

The access to the database server must be limited only the internal network which will be the authorized user only able to access the database server or configure it. This is to prevent unauthorized user from accessing the confidential data in the database and alter it.

For public access website that require a database to store information, the database must not be the same database as the internal network used. It must be a separated database which used to store public user data and information to prevent unauthorized user accessing the internal network employee’s confidential data and the company data.

The database must be backup at least once per day. If the unauthorized user able to alter the database like deleting the table from the database, there is a backup that will restore back all the loss data to prevent further damage to the company.

* **Network Security**

The company can place a server in between the entry router to use the server as an Intrusion Detection System (IDS) to monitor any malicious packet that flows in and out from the internal network and the entry point of the public network.

A honeypot can be used to trick the malicious user to thought that the honeypot server is the internal network server to monitor any malicious actions that the malicious user tends to do and log down the malicious user IP and details.

Firewall rules must be set that the firewall only allows the internal network user accessing the public network, but the public user traffic will be deny as they are not authorized to access the internal network services.

* **User Security**

In order the user to protect themselves, the password policy for the user must contains at least 2 special characters, length of password must be at least 10 characters with alpha numeric characters.

The user must not share the personal username and password to any unauthorized user to prevent any unauthorized access of company resources.

The user must not bring their own devices except their smartphone. If the user own device like their laptop are infected by a malicious user and the user connected their device into the company network, this might lead the malicious user to do a pivoting from the public network into the company network and access the company resources unauthorized.

* **Security Incident Handling**

The company must have their own security incident handling methods. If the company’s employee accidentally clicked into the malicious link which lead to malicious user accessing the company internal network, the incident response team must take action and notify the employee of the department to stop any actions from the pc the employee use. Then, the incident response team can start to monitor the logs of any malicious actions like routing the packet from the internal network to the public network, compromising the employee’s credential, injecting malicious program to infect other employee devices in the company internal network.

The incident response team must try to solve the employee’s compromised devices to prevent the malicious user to continue performing malicious actions. Then, the incident response team should analyze the whole problem and determine how the malicious user attacks into the internal network and create a report for it. Then, the team should decide how to solve the problem more efficiently fix all the problem that caused by the malicious user and think of a way to prevent that from happening again in the future.

* **Restrict services to your organization’s network/hosts**

To prevent employee to accidentally clicked into malicious website that might lead to attacker breach into the internal network. So to prevent this to happen, the administrator can only allows the employee to access to working related websites. Other websites like Facebook, Instagram should be block as some of the employee might accidentally clicked on the malicious link and this will be the main factor on the company internal network getting breached by the attacker.

* **Protecting Services that are allowed to internal network**

To protect the internal network from getting access by any unauthorized user, the administrator can use firewall software to only allows the internal network user traffic to transmit to the public network. With the helps of the firewall, we can prevent any unauthorized user from the public network from accessing the internal network.

If the employee wants to access into the company’s internal network, the company use Virtual Private Network (VPN) method to secure the connection to the company’s internal network. All the employee needs is the company VPN profile information with the credential to access the internal network. With this method, only the employee that have the credentials and the VPN profile information, so any unauthorized user would not be able to connect into the internal network if they do not have the credentials for the VPN connection.