**Denial of Service Protection Policy**

**Overview:**

Denial of Service (DoS) is a common cyber attack which floods the network ultimately, causing destruction in **comapny’s** workflow until fixed.

In order to prevent DoS attacks, the IT department will be implementing extra security measures to ensure that our networks and infrastructure are defended from such attacks.

As the IT department strengthens **company’s** networks it is also requested that employees implement good security practices to reduce risk as well.

This document will go in detail the measures the IT department and employees will be taking in order to ensure that the company network is secured.

**Network Security by IT Department:**

The following steps will clarify how the IT department will be strengthening our networks and infrastructure to prevent DoS attacks. Additionally, it will cover how the IT department will make plans to maintain a functional network that will be able to withstand DoS attacks.

1. Set up a defensive firewall.
   1. This will help secure our network by filtering and blocking out incoming requests that are not recognized by the system.
2. Closely monitor the network for suspicious behavior.
   1. The IT department will monitor network logs and other data to detect suspicious activity and take care of it in an appropriate manner when detected.
3. Disabling unused ports and services.
   1. Disabling what is not used or not commonly used will be able to help minimize the risk as it makes less flaws for attackers to find and attack from.
   2. This also helps the IT department be able to better keep track and secure the services that are being used.
4. Keep network information private.
   1. Information in relation to our networks and infrastructure will only be known to specific members in the IT department and shall not be shared with anyone aside from those employees.
5. Implement secure network infrastructure.
   1. This ensures that the network is up-to-date using proper and secure technologies to future minimize security risks in the network.
   2. In the event that there is a critical device on the network that has been attacked, there are also other devices that employees can rely on the network.
6. Have more than an adequate amount of bandwidth.
   1. In the event there is an attempted attack, the network will be able to handle more traffic than what it is normally used to with the additional bandwidth.

**Security Steps from employees:**

As the IT department makes security implementations, we ask that all employees also do their part to ensure that our network and infrastruc remains safe for use.

1. Implement secure passwords.
   1. Password Guidelines: Password is at least 8 characters long, containing letters (upper and lowercase), numbers, and special symbols such as (but not limited to) !@#$%^&\*()\_+-=.
2. Do not connect with unsecured WiFi networks.
   1. Unsecure WiFi networks pertain to public networks as well as unfamiliar networks.

In the case that there is a flaw found in our network and a DoS attack takes place, as an employee, please notify the IT department if you suspect that there is an attack taking place. If the IT department discovers the attack first, **company**  will notify all employees of the current situation and keep employees posted on the next steps following in regard to how the network will be fixed and how work will be conducted until things have been recovered.

If there are any questions or concerns in relation to the company’s DoS Protection plan, please contact the IT department at any point in time as they will be glad to assist.

**Sources:**

<https://www.giac.org/paper/gcwn/15/disable-nonessential-devices-services-reduce-exposure-dos-attacks/100301>

<https://us-cert.cisa.gov/ncas/tips/ST04-015>

https://www.esecurityplanet.com/networks/how-to-prevent-dos-attacks/

https://resources.infosecinstitute.com/topic/ddos-security-policy-template-prevent-massive-attacks/