The organization has a small, but growing employee base, with 50 employees in a tiny office. It's an online retailer of the world's most excellent artisanal, hand-crafted widgets.

The organization needs security measures to the following systems.

- An external website permitting users to browse and purchase widgets
- An internal intranet website for employees to use
- Secure remote access for engineering employees
- Reasonable, basic firewall rules
- Wireless coverage in the office
- Reasonably secure configuration for laptops

Active care for privacy also must be considered since the retail company is handling customer payment data. While the engineer still requires access to the internal website, along with remote, command line access to their workstations.

First, we need a security measure for an external website permitting users to browse and purchase widgets. To permit the users to browse and purchase widget, we must be able to identify the user.

Once an authentication system has been set up and the user authenticated, they may be able to purchase widgets. We also need to set up HTTPS on the external website; this guarantees that the user is talking to the server they expect and that nobody else can intercept or change the content they see in transit. We can also get web security tools and test our website security, which is pen testing. Setting up a limited number of logging attempt is also necessary.

Now that we covered some basic of security of the external website, now we cover internal security. Our employees also need to be authenticated so setting up an authentication system is necessary. The internal threat gets decreased by training employees on digital hygiene, for example advising all our employee not to interact with suspicious emails, and never open an email attachment unless they know what it contains and where to locate it. Testing our employee is also a good idea, by regularly testing our employee with a real-life scenario we get more insight on what is a common attack vector and alert us to areas where our employees might need further education. We also need to tighten overall network security, all logins need to expire after a period of inactivity, passwords need to change regularly, and we need to ensure that all passwords are strong (Must include uppercase, lowercase, unique character and is at least 8 lengths long) and never written down. They are locking the screen down when the employee takes a break.

The engineers need secure remote access. For secure remote access to happen, a strong password is required, and a proper authentication system must be set up. The software that provides the remote service must always be up to date. Restricting access using firewalls is also recommended. We then must enable network level authentication and limits user who can log in using remote desktop. Then we set an account lockout policy which limits the number of loggings attempts. The engineer should also apply the internal security policy that we suggested.

Now we need some basic firewall rules, let's start with documentation, we need to minimum keep track of the purpose of the firewall rule, the service it affects, the user and device it affects, the date of the rule, when the rule expires and the name of the person who added the rule. Then we need to establish a formal change procedure since firewall rules need to get updated for any new services and new devices that get added — for example, a change request process for users to request modifications to a specific firewall configuration. A review process to analyze these new modification requests and determine the best course of action for any security practice. A process to test the new modification requests on the production firewall rules. A process to validate the new firewall settings to ensure proper operating and a documentation process to track the change that gets made. We also need to block traffic by default and only allow specific traffic to identified services. Logs must get frequently audited so that we can know which use it has overall and know if a threat has emerged. The rule of the firewall needs to get reviewed regularly. Our network is always changing; we are gaining and removing users and devices. That means news application and new services. All those changes need new firewall rules. As always, our firewall software and firmware must always be up to date. All this change must get communicated with the right people and at the right time.

To cover the office with wireless internet. We must first employ the router with WPA2 with AES/CCMP. We need a long and complex password with a unique SSID. Now the attackers require to do the computation themselves, increasing the time and resources required to pull off an attack. WPS also must be disabled. So, we must make sure that this feature is disabled on our AP's Management Council. We recommend checking that this kind of feature is disabled using a tool like Wash; some router manufacturers don't allow the user to disable it.

Setting up a VLAN is recommended. If we segment a large LAN to smaller VLANs, we can reduce the broadcast traffic as each broadcast will be sent on to the relevant VLAN only. VLAN also provide enhanced network security. VLANs gives network administrator control over each port and user. A malicious user can no longer plug their workstation into any switch port and sniff the network traffic using a packet sniffer. It is also cheaper by segmenting a larger VLAN to smaller VLANs than creating a routed network with routers because normally routers cost more than switch.

We now need some secure laptop configuration. Some of the things we must ensure, that the laptop should get configured so that the password must get entered every time we turn the machine on or when it comes out of hibernation, sleep or screensaver mode. The password always must be complex and lengthy. We must disable booting from CD or USB and encrypt the hard drive, to stop the thief from

stealing the data when the laptop gets stolen. Using a VPN is also recommended this stop hacker to from eavesdropping on emails or copy passwords as they pass over the network when we connect to a public network. Using the secure email that uses a secure socket layer or transport layer security is also recommended since the VPN won't always work. The laptop must always be updated with the latest firmware and software; this security patch is incredibly essential. A good backup policy for the laptop is also needed, in case of corruption or when you delete something accidentally. The laptop should never be left unattended. An inventory system is also needed so that we can keep track of who has a company laptop, and what they're doing with it. The personal laptop should never be allowed on a company network.

The company also need to have a good application policy. This policy serves to support, and they define the boundaries of what applications are permitted or not, but they also help educate folks on how to use software more securely. One of the recommendations is only to support or require the latest version of a piece of software and making sure that all security patches get applied and the most secure versions are in use. It's also a good idea to disallow risky classes of software by policy. For example, things like file sharing software and piracy-related software tend to be closely associated with malware infections. We need to define a policy around what type of software can be whitelisted; for example, a video game does not need to be whitelisted since this company makes widgets. Browser extensions or add-ons is also something to think about.

Now finally, let's go over privacy since this company is handling the customer payment data; having strong care for privacy is important. We need privacy policies that prevent customer data from external threats and misuse by employees. We need periodic audits on cases where sensitive data was accessed. Strong privacy rule is super important, because it helps us ensure that sensitive data is accessed by people who are authorized to access it, and they use it for the right reason. We should apply the principle of the least privilege, by not allowing access to this type of data by default. They need to first to make an access request with justification for getting the data, the request needs to get specified on what data they need access to, and it needs to have a time limit that needs to be called out in a request. The customer data should also always be encrypted. One of the things we need to do is set up an IDS(Intrusion Detection System) and an IPS(Intrusion Prevention System). This actively triggers warning and block malicious traffic if they see something suspicious is trying to access customer data.

Source:

https://www.liquidweb.com/kb/best-practices-for-firewall-rules/

https://www.esecurityplanet.com/network-security/finetune-and-optimize-firewall-rules.html

https://en.wikipedia.org/wiki/Wireless_security