UNBOUND™

Technology Guide

TABLE OF CONTENTS

1 Physical Equipment

- Using computers of all the same brand may simplify maintenance and support.
- As of January 24, 2020, Windows 7 is no longer supported or updated by Microsoft. It is recommended to update all computers to Windows 10. It is no longer secure to access the internet using Windows 7.
- With Windows 10, a minimum of 8 GB of RAM is recommended. If an older version of Windows is used, 4 GM minimum is recommended.
- Processors in the "i" series are recommended at a minimum, for example, intel Core i5, i7, etc. Older Pentium processors are not recommended.
- It is recommended to set Windows updates to apply automatically. There should be a verification system in place to make sure automatic updates are applied to each computer, even if it is a manual check of each one.
- Maintain an inventory listing of all computers.
- When PC hard drives stop working or are disposed of, take precautions to destroy them (not just to delete the information but to destroy the hard drives physically, such as by shredding them, so the information cannot be accessed). Any step that renders the hard drive non-functioning and non-readable is sufficient. If a vendor is used to do this, request that you can watch the hard drives being destroyed or request documentation showing what was done.

2 User Access

- Make sure that computers are password-protected. If multiple users use the same computer, each user should have their own password to the computer. Passwords should not be shared among users.
- Create a password complexity policy, such as requiring passwords to have a mix of uppercase and lowercase letters, numbers, etc.
- Require passwords to be changed on a regular basis, such as every 90 days.
- Consider only allowing users to have administrative access to computers if needed. If any users do have administrative access on their computers, review the computers regularly to make sure the programs being downloaded are appropriate and needed for work at Unbound.
- Consider creating a policy that discourages users from using the Internet for personal things. Specific or inappropriate websites can be prohibited if needed. Occasionally check browser history to ensure inappropriate websites are not being visited, as this can create a potential of downloading something malicious.
- Consider offering general computer training to users, such as on Windows or specific programs.

3 Network

- If a network is used to connect computers, audit the network connection periodically to ensure no one is using it other than Unbound staff. When someone leaves Unbound, terminate their access to the network.
- If a network is used, use a firewall to prevent unauthorized access.
- Do not connect to untrusted public networks, for example, wireless networks available in internet cafes or airports using Unbound computers or accounts. For example, do not access an Unbound email account while connected to an untrusted public network. It is possible for others to access information over public networks. If a trusted Virtual Private Network (VPN) is used while connecting to public networks, then the connection may be secure.

4 Data Backups

- Data should be backed up, based on its importance, based on its criticality to your operation. Ask questions such as "if we lost this data, what damage would be done?", or "How long can we be down if our systems crash or we lose data?" or "How often does this data change?" The answers to such questions will help you decide how frequently you should perform data backups.
- An online storage service like Microsoft OneDrive or Google Drive maybe be a good fit that does not require a lot of technical setup. This is recommended over USB or other external drives, as they are subject to hardware failure.
- Review the data backups manually on a regular basis to ensure that the backup is working well (that the data are not corrupt or unusable).

5 Internet

- If you are working online always make sure the website URL is using "https" rather than "http" - the "s" indicates a secured site.
- Do not share website passwords with other users. Each person should have his/her own unique password.
- When available and not cost-prohibitive, purchase an Internet connection that is fast enough to keep users from encountering delays with their online work.

6 Antivirus Software

- There are many antivirus applications that work well.
- If a network is used, the key is to centrally manage the computers on your network in order to prevent malware and also be notified in the event of a threat. In a centrally-managed network, you can remotely verify which computers are up-to-date
- If the computers are all standalone rather than connected to a network, setting the antivirus software to auto-update is critical. With standalone computers, you would need to periodically check them individually to ensure they are staying up-to-date.
- If a computer is infected and the antivirus does not handle it properly, it would be ideal to turn it off, unplug it from the network, and reinstall the operating system. If the antivirus does handle the threat, it is a good idea to scan the computer again to make sure there are no more threats.
- For Windows 10 computers, "Windows Defender" which comes bundled with Windows 10 is a good solution and comes at no additional cost. For a centrally-managed environment, pay-for enterprise solutions may be a better option. Depending on what is available in each country, this could be a solution offered by companies like Eset, McAfee, Kaspersky, or several others (please consult your local technology vendor to determine what solution is available in your country).

7 Other Software

- Make sure all software licenses, including Microsoft Windows, are legal. Microsoft may offer you a significant non-profit discount on their products if you contact them at Microsoft.com
- Keep an inventory of software licenses to ensure all copies are legal.
- Software should no more than 2 versions behind the most recent version available and should still be supported by the manufacturer. For example, if the most recent software version published is 5.4 and the previous versions are 5.3, 5.2, 5.1, etc., the version on each computer should be at least 5.2.
- Restrict access of custom software to only the users who need it. Ensure that each user has a unique account and password that is not shared with other users.

8 Information Privacy

- For the personal information of employees that is stored either digitally or on paper, make sure that it is only available to staff who need to know this information. Take precautions to secure the data. Any data stored digitally should be password-protected. Data stored on paper should be securely locked.
- The personal information of sponsors that visit the project should be secured and only accessed as needed. After a trip is completed, this information should be deleted (if digital) or shredded and disposed (if on paper).
- If there are data privacy regulations specific to your country, make sure you are complying with them. (For example, in the United States, we are required to store credit card information of sponsors in very specific ways.)

9 Computer Maintenance

- If a computer is running slower than expected, you can use Task Manager, built into Windows, to see what applications are taking up the computer's resources. It is possible a computer needs its operating system reinstalled if users continue to have problems. If the hard drive space of the computer reaches 90% or fuller, the performance of the computer will degrade, so deleting files to free up space may help its performance.
- The air vents of computers need to be unobstructed. In dusty environments, the interior may need to be cleaned.
- Computers can be left powered on overnight, but make sure users at least sign out of the computer and it is left on the Windows lock screen. Doing a daily restart on a computer is always a best practice, either at the beginning of the day or at the end of the day when signing off.

10 Information Security with email and mobile phone use

- Never click on a link or open an attachment in an email if it is not completely certain that the link or attachment is secure. Clicking on these items can give a malicious person access to the network or confidential information or infect the network with a virus.
- Advise families what information they can expect to receive from Unbound via mobile phone or email, for example, an eLetter or a request for a photo, and how these messages will appear. Advise that them if they receive other messages (for example, a request to meet or for personal or bank account information), that they should not respond. They should contact Unbound staff to report the request.
- Do not accept calls or click on links in messages from unknown people.
- Review the privacy settings in WhatsApp – control who can see your photo, status and other information.
- Encourage parents to review the mobile phone activity of their children and to talk with them about security.