DANENET TECHNOLOGY WITHIN REACH

RECOMMENDED TECH PRACTICES

OVERVIEW & PURPOSE

This document is a tool for DANEnet clients and other nonprofits to use when reviewing technology practices and planning. It is not intended to be comprehensive, but an overview of important practices and considerations.

Contents

Network infrastructure understanding

Minimum	Better Practices	Tools and resources
Know who your Internet provider is and the location of service entry. Know where your modem, router and switches are located. Document your router username and password. Have a plan in place for what happens if the Internet isn't working.	Diagram internal network and document IP addresses. Label all network equipment. Designate a network administrator or Global Administrator/Super Admin. Minimize use of switches throughout space.	Angry IP Scanner can provide a list of devices on your network

Software / Operating System (OS) currently under support

Minimum	Better Practices	Tools and resources
OS is updated daily as updates are available. OS should be retired before it is out of extended support. Maintain software license information, including login information for the MS Open License website.	Plan for OS replacement/upgrade before mainstream support has ended. Automate the OS update process. Consider virtual servers with distributed tasks and complete hardware independence.	Windows Lifecycle Fact Sheet https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

 use freely but please credit our work.

Skilled staff and training

Minimum	Better Practices	Tools and resources
Designate someone to be a tech manager; in a larger organization it should be a significant part of someone's job description. Provide staff training on mission critical technology tools and software (i.e. database data entry, attendance tracking).	Technology manager responsibilities include: keeping track of credentials, be trained on simple tasks (toner in copier, power cycle router, etc), be the specified contact with your tech support vendors, be able to add and remove users and hardware.	Techsoup webinars Idealware training calendar Nonprofit Technology Certificate Product specific training and certifications

Password / account management system

Minimum	Better Practices	Tools and resources
At least 8 characters with some complexity (things like uppercase, lowercase, number or symbol). Passwords should not be posted or visible. Longer passwords are better passwords. Passwords should be memorable and/or managed.	Avoid words related to the user, agency or mission. When possible use a phrase or group of random words totalling at least 20 characters. Change annually. Use a password manager or encrypted storage. Protect passwords that control a critical resource or service with encryption.	KeePass: https://keepass.info/ LastPass: https://www.lastpass.com/

Control over brand, domain and credentials

Minimum	Better Practices	Tools and resources
Know credentials for your domain registrar and domain host, set up auto-renew. Administrative email is up to date and monitored. Register trademarks if needed. Know the location of your DNS records.	Carefully consider domain name before registering (long email addresses can be a hassle). Keep an offline copy of your DNS records.	MX toolbox: https://mxtoolbox.com/ Whois: https://whois.icann.org/en

 use freely but please credit our work.

Protection from viruses and malware

Minimum	Better Practices	Tools and resources
Run built-in antivirus/malware program (Windows Defender/Security Essentials) and keep it updated. Use freeware antivirus or anti-malware software. All staff have training / knowledge to avoid technology scams and malware.	Local users do not have administrative privileges on their workstations. Paid subscription to a top-tier antivirus product. Malware removal tools installed on workstations and run monthly.	Free: Windows Defender/Security Essentials, Bitdefender Free, Panda Free, Avast, Malwarebytes Paid: Bitdefender or Symantec at TechSoup, Vipre Antivirus for Business (50% discount), ESET Secure Business (64% discount)

Technology needed for your organization to work effectively

Minimum	Better Practices	Tools and resources
Replace inefficient hardware. Replace software before it is no longer supported. Get an Internet connection fast and reliable enough to suit your needs. Replace hardware before it dies.	Keep subscriptions or software assurance active. Plan and budget for hardware and software upgrades. Keep up with new technologies available to help better serve your organization's mission or workflow.	Techsoup www.techsoup.org Check for nonprofit discounts with other venders Idealware www.idealware.org/

Resource allocation, planning and technology policy

Minimum	Better Practices	Tools and resources
Think about what technology your employees/volunteers need to do their jobs and what technology your users spend most of their time using. Your mission and people should drive technology decisions. Have organizational policy for acceptable use.	Budget for ongoing technology maintenance, upgrades and inevitable tech problems. Actively seek out better technologies for your organization. Develop a technology plan. Have organizational policies for bring your own device, IT security, disaster recovery, data storage and social media. Strategic plans include technology.	Consider online tutorials, review plans with your technology consultants, attend pertinent seminars. Engage Board or advisory committee in technology planning

 use freely but please credit our work.

Backup

Minimum	Better Practices	Tools and resources
Daily backup of critical data to an external drive. Backup jobs are monitored for success and failure. Tests are done on a quarterly basis to verify ability to restore.	Automated full system backup to local external drive and offsite location (cloud). Backup is monitored daily and tests are done on a monthly basis to verify ability to restore.	At minimum, use built-in system tools (i.e. Microsoft Backup, SQL Backup, etc.) Or better, use Cloud backup solutions (i.e. Cloudberry, Altaro)

Email

Minimum	Better Practices	Tools and resources
Access email where you need it. Be able to regain access to accounts if the password is lost. Have a policy and procedures for what happens with new and departing users.	Have email at your own domain (not a @gmail.com, @yahoo.com, @tds.net account). Sign up for Google's G Suite for Nonprofits or Microsoft's Office 365 offerings.	Google for Nonprofits: https://www.google.com/nonprofits/ Microsoft 365: https://products.office.com/en-us/nonprofit/office-365-nonprofit

Internal Security

Minimum	Better Practices	Tools and resources
Restrict access to your physical server and to sensitive data. Do not share or post passwords. Encrypt on-site backups.	Establish restrictions for any guest access. Avoid shared accounts - each user should have their own access to resources and data.	Use Active Directory or Office 365 Dashboard to add new users

Better Practices Checklist

- ❑ Diagram internal network and document IP addresses
- ❑ Network equipment is labeled
- ❑ Global / Super Admin is designated
- ❑ OS is in support and automatically updated
- ❑ Virtual servers are used as practical
- ❑ Designate a tech manager or similar position
- ❑ Provide staff training on critical technology tools
- ❑ Use of long passwords that change annually
- ❑ Use of a password manager or encrypted storage
- ❑ Location of DNS records known and offline copy kept
- ❑ Credentials for domain registrar and host are known and not allowed to expire
- ❑ Local users do not have administrator privileges
- ❑ Use of top-tier anti-virus product
- ❑ Malware removal tools installed on workstation and run monthly
- ❑ Software subscriptions and assurances are active
- ❑ Research, evaluate and use new technologies to help you work better and achieve your mission
- ❑ Plan and budget for technology
- ❑ Have organizational policies for: 1. Acceptable use 2. IT security 3. Disaster recovery 4. Work product / filing standards
- ❑ Strategic plans include technology
- ❑ Automated full system backup (local and offsite)
- ❑ Backup is monitored daily and tested monthly
- ❑ Have email at your own domain
- ❑ Each user has access to own data and resources

 use freely but please credit our work.