DIGITAL TECHNOLOGY AUDIT TEMPLATE

This template covers the basics of the organisation's operational or "back-office" technologies. It is purely to be used as a basis for benchmarking existing technology (hardware, software, back up and disaster recovery, licensing and support.)

Undertaken by ……
Date……

1. Overview

e.g. An audit was undertaken of …….. on ……., including ***a diagnostic test of each computer or mobile device on the network or owned by the organisation****, and an* ***individual questionnaire with available staff.***

2. Technology Overview

A summary of the following should be made after the completion of the audit.

2.1. Hardware

2.2. Software

2.3. Networking and Security

2.4. Policies and Procedures

2.5. Webpresence, email, and intranet

2.6. Cloud apps

2.7. Information and data

2.8. Training

2.9. Back-up and disaster recovery

2.1. Hardware

Give details of the hardware in the office and owned by the organisation, including memory and any performance issues. You may want to use a diagnostic tool such as Belarc (www.belarc.com). Give details of server and peripherals (e.g. networked printers, standalone devices such as cameras and scanners, 3G phones and tablet devices, etc.)

2.2. Software

Licensing status of software; how users are set up to access software (e.g. as administrators); standard software set up (E.g. windows updates); version(s) of software inc. operating system and office software; specialist software; virus protection; server software inc. any backup software. Collect administrative passwords for all organisation owned devices.

2.3. Networking & Security

Type of network, inc. wired and wireless; broadband connection bandwidth availability – you may want to use a speedtest to check the connectivity your organisation actually receives. ("Up to 8MB" does not mean that you get 8MB of connectivity all of the time. Run a speedtest at lunchtime, when your staff and staff in offices near you will be online surfing). http://www.speedtester.bt.com/

You may have more than one "network" (e.g. public and private); shared drives (or P2P) for storing data; virus protection; firewalls; etc. You might want to establish a network diagram, and create a list of router passwords.

2.4. Policies & Procedures

This is a generic list of good practice policy and procedures (please amend as appropriate)

a. Contacts and contracts with suppliers should be held in an accessible place, (paper copy) and a number of staff should be aware of them, and what is covered.
b. All computers should be checked at least once a month. This might include running Belarc Advisor, downloading the latest software updates (Windows updates are issued on the 2nd Tuesday of each month, mac software update should automatically update the user), ensuring antivirus is up-to-date, and basic maintenance (e.g. clearing cached files using Disk Clean Up.
c. Servers in house should be backed-up on a nightly basis and the tapes should be held securely off-site if possible, or in a fireproof safe. Other computers should also be backed-up as appropriate, either to local hard drives, or online back-up facilities like http://www.crashplan.com. Both is best.
d. All software should be licensed and details of licences should be held centrally. Windows operates a "Genuine Advantage" programme which only recognises licensed software.

e. It is advisable that all hardware has a security code written on it, and is listed in an asset register, maintained centrally.
f. It is advisable that an organisation has some guidelines around "fair use" policies for using the internet, accessing mail, downloading software and storing files. However, this should be based on organisational needs – if you have great bandwidth then you won't need a fair use policy for watching videos at lunchtime. An organisation might want to specify what sort of content can be accessed on the work network, and what can be downloaded and kept on work servers/storage.
g. "Shared hardware" (e.g. laptops, tablets, digital cameras, USB dongles, etc.) should be accessible centrally and be controlled by a booking form or logbook.
h. Staff should be aware of Data Protection and Freedom of Information legislation as it applies to them.
i. Websites should have terms and conditions and disclaimer information readily available. Websites that include User Generated Content need different Terms and Conditions and Privacy Policies. Search http://getambition.com/resources for these. All websites should comply with the Disability Discrimination Act. Since May 2012, websites also need to comply with EU Cookie Legislation: http://www.getambition.com/2012/04/are-you-ready-for-the-cookie-law/
j. Since early 2007 emails are legal documents and therefore should have company address information as standard for their email signature. You may also want to set a company policy on the sort of communications appropriate for email (for example, "Do not send negative communication by email, either internally or externally").
k. When creating digital content with others that your organisation plans to use digitally, you must ensure an Image/Content release form is signed. There is a specific set of rules relating to children and digital content – see Own-IT's Child Protection factsheet http://www.getambition.com/resources/own-it-child-protection-and-digital-content-factsheet/. Do you have these forms available for staff and do they know when they need to use them?
l. A technology plan will enable the organisation to plan software spending and will include a replacement policy, for upgrading machines, usually on a 3-5 year cycle. Laptops may need to be replaced every 2-3 years depending on how much they travel about.
m. Many of these policies should feed into a company-wide Disaster Recovery/Contingency Plan.

2.5. Webpresence, email and Intranet

It is useful to have a brief overview of web, email, and intranet as part of your technology plan, however if you are looking to redevelop any/all of these this will be a separate piece of work. In relation to your webpresence:

Website:

Make a note of all information needed to contact….Hosting provider; domain name(s) and registrar; developer; content management system; who has administrator privileges (and other privileges); any annual or ongoing costs; 3rd party plug ins (e.g. box office, e-commerce, Paypal) ; intranet; email addresses. List any statistical analysis packages you use with log in details (eg. Google Analytics)

Other webpresence:
List other places your organisation has a webpresence with full account details (username and password) and a note of who is responsible for updates and if you have any policies for using them: eg. Facebook; Twitter; listings aggregators; other blogs you comment regularly on; etc.

Email
List who hosts your email, and how mailbox sizes, diverts and out of office autoresponders are set. What's your policy for archiving email? Do staff understand how to link mobile devices to their email if they need to? Do staff have webmail log ins?

Intranet
You might still run an intranet if you have your own server on site. What drives are for what information? Who cleans it up/backs it up/updates it?

2.6. Cloud apps

What apps do you use on the cloud? List, with any log ins and policies for use: project/task Management apps, document and file sharing, photo and video storage, shared diaries and milestones, CRM systems, e-newsletter apps, event booking apps, back up systems, etc. Most cloud apps are paid for monthly, so which credit card is used, and when's its expiry date?

2.7. Information & Data

What data you store, what data you use, what you have to provide for funders etc., mailing lists etc. Where is the data stored? How do you collect the data? Do you share any of it? What are the permissions you seek? Do you syndicate any of it or provide an API to allow access to it? You may need to do a separate information audit alongside the technical audit if your organisation collects a lot of data. This is a useful guide about how to protect data whilst still being open and transparent. http://www.getambition.com/2009/12/how-to-syndicate-your-data/

2.8. Training

List staff skills and staff training needs on operating systems, key software applications and familiarity with hardware systems. Also establish social media familiarity and skills and work out whether staff know how to sync their data between machines/mobile and tablet devices/back up systems.

2.9. Back-up and disaster recovery

How is each machine backed-up? How is the server backed-up? How are machines "on the road" backed up? What happens if any of elements fatally crashes? What is the procedure for reinstating lost data? We recommend that all systems should be backed up daily, both remotely (to somewhere online) and locally (to a hard drive in the organisation, or attachable to a laptop). What happens if you lose power in the venue? What happens if you lose internet connection? With most box offices now being run online, these are business critical pieces of information, and all staff need to know what the process is for ensuring business can continue.