# ICT Security Guide for Technical Staff

## Introduction

Qatar schools are vulnerable to cyber-attacks, putting student, employee and administrative data at risk. The conclusion is based on reported security incidents from Doha's National and International schools. This is very alarming, considering the amount of personal information on staff members and students these networks contain.

Examples of confidential data that could be compromised are financial records, payroll data, student's medical files, exam results, bus routes ...etc.

## What is Information Security?

Information security is the process of protecting information and protect its confidentiality, integrity and availability.

## Why is Information Security Important?

- Ensuring that your information remains confidential and only those who should access that information can.
- Knowing that no one has been able to change your information, so you can depend on its accuracy.
- Making sure that your information is available when you need it
- Secure information and communication technology environment will promote collaboration among teachers, students, parents, administration, venders and partners by providing them controlled network access.
- Improving productivity by ensuring network uptime and by recovering quickly from security breaches.
- Enhance your customers and client's satisfaction by allowing them to access confidential information on your network applicable to them.
- Provide teachers with secure access to manage their classes

## Goals of Information Security

- **Prevention**
  Prevent computer or information violations from occurring. The better your prevention policies, the lower the likelihood of a successful attack occurring.

- **Detection**

Identify the assets under attack, how they occurred, and by whom. Detection activities should be ongoing and part of your information security policies and procedures.

- **Response**
  Develop strategies and techniques to deal with an attack or loss and a plan to respond, restore operation, and neutralize the threat.

## What are the risks?

Many schools now are greatly depending on information stored in computers. Personal staff details, salaries, financial records AP/AR, students registrations, test results, bus schedules, marketing information and students medical records may all be stored in a digital format on multiple computers. Information can be stolen (confidentiality) or modified (Integrity) or becoming inaccessible (Accessibility). Without this information, it could be very hard for a school or small business to operate. The effect on reputation and the risk of litigation could be devastating if confidentiality was compromised. Consider the harm that could be caused if a competitor retrieved students/parents information.

Information security systems need to be implemented to protect this information.

## What are the threats?

- **Viruses**
  Viruses are malicious software that inserts malicious code into existing documents or programs, and then spreads itself by various means. Viruses are still by far the most common type of network security threat.

- **Trojan horses**
  It is malicious software that disguises itself as something innocent once installed on a computer it will open a back door to allow access to the system.

- **Spam**
  Spam emails designed to trick recipients into clicking on a link to an insecure website. Spam email takes a variety of forms, ranging from unsolicited emails promoting products to coordinated spam attacks designed to take up so much bandwidth on a network so as to cause it to crash.

- **Phishing**
  Phishing refers to spam emails designed to trick recipients into clicking on a link to an insecure website. An example of a phishing email will supply you with a link to click on, which will take you to a page where you will be asked to re-enter all your bank account details, including credit card number(s) and/or

passwords. Of course, these sites aren't the actual bank's site, even though they appear similar.

- **Exploited vulnerabilities and Zero-day exploits**
  These are "bugs" in operating systems and software that can be exploited by hackers. When a vulnerability is discovered, the race begins: hackers hurry to develop exploits, which are pieces of code that use the vulnerability to penetrate or disable a program or a whole network, before the software developer releases a patch to close the hole. Zero-day exploits are when an attacker can compromise a system based on a known vulnerability but no patch or fix exists.

- **Insiders**
  Insiders can be broken down into three categories: careless & untrained employees, employees that are duped or fall prey to social engineering type attacks, and malicious employees.

- **Loss/Theft of Mobile devices**
  Theft is still a major cause of data breaches as mobile devices. Tens of thousands of mobile devices are stolen each year and often these have sensitive data that require public disclosure as a data breach.

- **Social networking**
  Social networking sites such as Facebook, MySpace, Twitter and others have changed the way people communicate with each other, but these sites can pose serious threats to organizations. Social networking sites are breeding grounds for SPAM, scams and a host of other attacks.

- **Social engineering**
  Social engineering is always a popular tool used by cyber criminals. It is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques.

- **Zombie Computers and Botnets**
  A 'zombie' computer is a computer infected with malware that causes it to act as a tool of a spammer by silently sending out thousands of emails from the owner's PC. Infected 'zombie' computers, are organized by hackers into small groups called 'botnets'.

- **Inappropriate or Illegal Content.**
  Though not considered a security threat, inappropriate content can seriously damage students and employee productivity. Web sites with illegal content often contain files with viruses, worms, and Trojans horses embedded in the available downloads.

# How Vulnerable is My Network ?

Vulnerability assessment is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure. Vulnerability analysis can also forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.

## What to do

### People

- Never download anything in response to a warning
- Update software regularly
- Use strong passwords and keep them secret
- Don't put an unknown flash drive into your PC
- Be very cautious about opening attachments or clicking links in email
- Avoid clicking 'Agree', 'OK', or 'I Accept' in banner ads
- Only download software from websites you trust
- Never turn off your firewall
- Always backup your data

### Process & Policies

Policies are certain rules that are meant to keep data safe and the business running smoothly. A security policy should consist of various rules and instructions, such as a password policy, requiring users to have passwords that cannot be easily guessed or broken and firewall rules permitting specific traffic in and out of the network.

### Technology

#### Network design

Some areas you need to consider are the types of nodes, user groups, security needs, population of the network, applications used, and the network needs for all the interfaces on the network. When designing or upgrading your network, you need to keep some basic rules of segmenting in mind. You need to segment your network primarily to relieve network congestion and route data as quickly and efficiently as possible.

### VLAN
Virtual LANs can be used to break up broadcast domains in layer 2 switched networks. Routers are still needed in a layer 2 virtual LAN switched internetwork to enable the different VLANs to communicate with each other.
In a flat network, all users can see all devices. You cannot stop devices from broadcasting or users from trying to respond to broadcasts. Your only security consists of passwords on the servers and other devices.

### Firewall
A firewall acts as the security guard between your network and the Internet. The main purpose of a firewall is to keep out unwanted traffic, such as a computer worm attempting to infect computers with a specific vulnerability. Note that some firewalls can also be used to block specified outgoing traffic, such as file sharing programs.

### Antivirus
Antivirus software is used to scan files on the computer on which it is installed, files that are downloaded to the computer, and emails. In addition to implementing Antivirus solutions on each machine, it is important to have an Antivirus gateway, a local or remote machine where email messages are scanned for viruses while they are being downloaded to the client computer. It is crucial to keep the antivirus software updated at all times, as new viruses are found almost every day.
Do not forget that simply having the software is not enough. Schedule an automatic scan if possible. Otherwise, then set a reminder to ensure that users run the scan on their computers periodically.

### Patches and Updates
Software vendors provide updates that are meant to fix bugs and patch potential security holes in their software. Make sure you regularly check for updates.

### DMZ
A Demilitarized Zone (DMZ) is an area where you can place a public server for access by people you might not trust. By isolating a server in a DMZ, you can hide or remove access to other areas of your network. You can still access the server using your network, but others are not able to access other resources in your network.

### Authentication
Authentication proves that the user or system is actually who they say they are. Authentication systems or methods are based on one or more of these three factors:

- Something you know – a password or PIN
- Something you have – a smart card or an identification device
- Something you are – your fingerprints or retinal pattern

## Backup

A regular schedule of backups for both software and data should be in place.

- Validate software and data before backup.
- Validate software and data after backup.
- Verify the ability to restore from backups.

## How to know your Computer/Network has been compromised

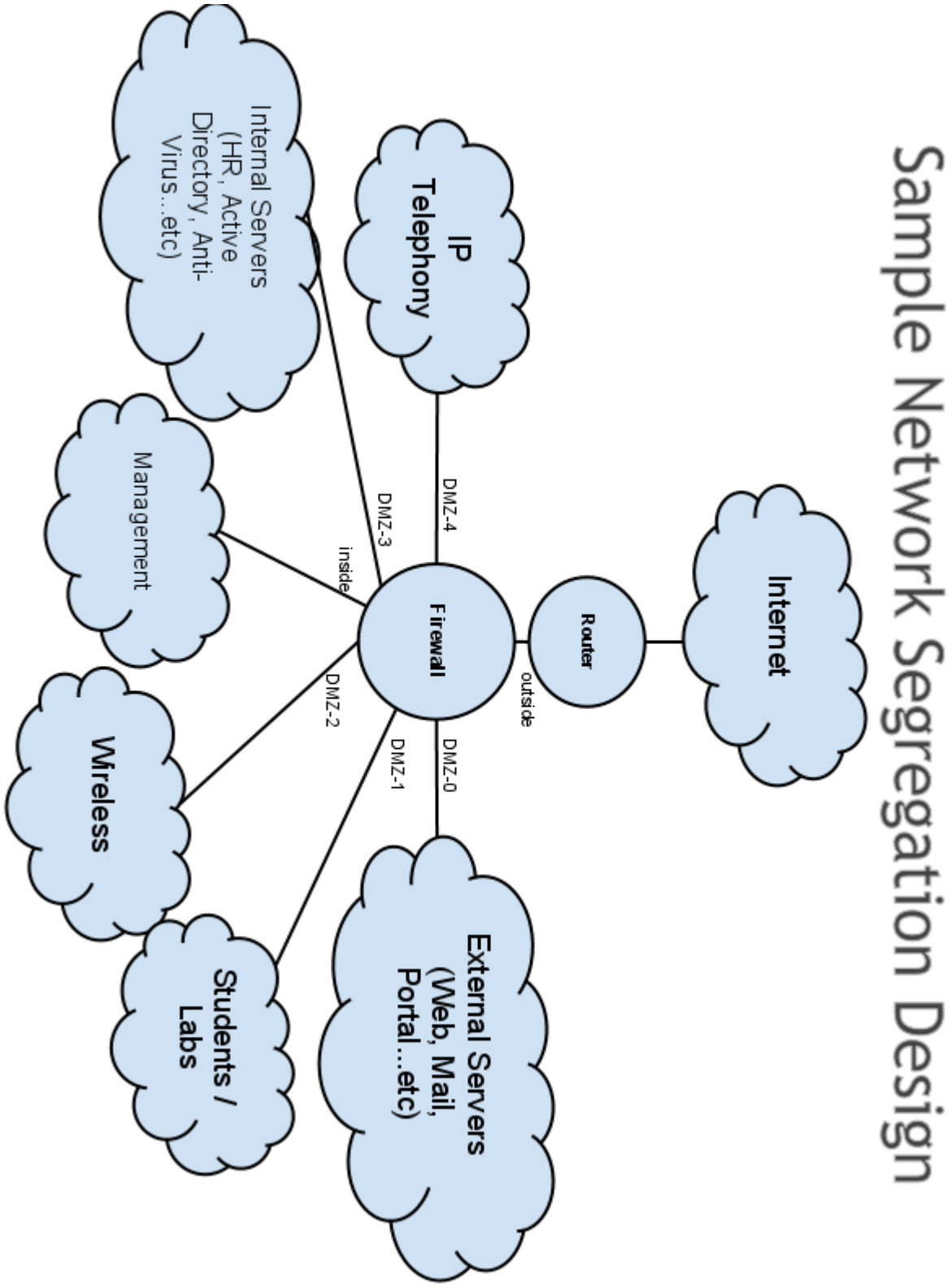
- Look at your antivirus icon to make sure that it hasn't been disabled. Press the "update" button and make sure that the program can accept updates.
- Keep track of whether the hard drive light flashes continually even when you're not using your computer.
- Consider whether your computer is slow or non-responsive.
- Check for unusual log entries
- Check whether it's running programs that you're unfamiliar with.
- Your screen is showing a window alerting you that your computer has run out of disk space unexpectedly. Another sign of a compromised computer is not being able to run a program due to not having enough memory.
- Exercise caution if you enter your password correctly and it gets rejected.
- Take note of the following symptoms: an email bounces back, you can't receive email, or employees' passwords don't work. Additional symptoms include complaints from users about to the network's slow response or new processes running on the server.

## What to do

- Disconnect the infected machine from the network to prevent further damage.
- Backup or image the computer's hard drive (so as to recover the important data later)
- Perform a clean install of Operating System - a format of the drive **must** be completed.
- Immediately update that installation with all of the latest patches.
- Use the latest anti-spyware, anti-virus, and event rootkit detection to scan and clean any data that you want to recover from the backups

## Information Security best practices

- Use an Internet firewall.
- Keep software up-to-date, preferably by using automatic update features.
- Run up-to-date antivirus software.
- Run up-to-date antispyware software
- Education and Awareness Increase awareness among your workers.
- Physical Security Control physical access to information assets and IT services and resources.
- Continuity Planning & Disaster Recovery Develop business continuity and disaster recovery plans for critical assets and ensure that they are periodically tested and found effective.
- Use appropriate monitoring, auditing, and inspection facilities and assign responsibility for reporting, evaluating, and responding to system and network events and conditions.
- Vigilantly monitor the content of your inbound and outbound campus e-mails and monitor visited websites to make sure no viruses, spyware, malware, or other malicious threats can infect your network. Prevent employees from visiting sites with illegal or offensive content.
- Deploy security hardware and software offered by a vendor with the financial and technical wherewithal to continually develop, test, and improve its security solutions.


Sample Network Segregation Design
Internal Servers (HR, Active Directory, Anti-Virus..etc)
IP Telephony
Management
Wireless
Students / Labs
External Servers (Web, Mail, Portal...etc)
Internet
Router
Firewall
DMZ-4
DMZ-3
DMZ-2
DMZ-1
DMZ-0
inside
outside

| | |
|---|---|
| **Anti-Virus engines** | |
| Microsoft Security Essentials | www.microsoft.com/security_essentials/ |
| Avira | http://www.avira.com/en/avira-free-antivirus |
| Panda Cloud | http://www.cloudantivirus.com/en/ |
| AVAST | http://www.avast.com/free-antivirus-download |
| **Personal Firewall** | |
| Comodo | http://www.comodo.com/home/internet-security/firewall.php |
| **Flash disk Protection** | |
| USB Immunizer, Bitdefender | http://labs.bitdefender.com/?page_id=108 |
| USB Vaccine, Panda | http://research.pandasecurity.com/Panda-USB-and-AutoRun-Vaccine |
| **DNS Security** | |
| OpenDNS | http://www.opendns.com |
| NortonDNS | http://nortondns.com/ |
| Comodo Secure DNS | http://www.comodo.com/secure-dns/switch/ |
| **Patch / Vulnerability Management** | |
| Secunia Personal Software Inspector | http://secunia.com/vulnerability_scanning/personal/ |
| UpdateChecker | http://www.filehippo.com/updatechecker |
| **Network Security software** | |
| Aastaro Security gateway | http://www.astaro.com/landingpages/en-worldwide-homeuse |
| **Web Filtering** | |
| OpenDNS | http://www.opendns.com |
| Email Filtering | http://www.google.com/apps/intl/en/group/index.html |
| **Encryption** | |
| Disk Encryption | http://www.truecrypt.org/ |
| online text encryptor | http://www.alltextencryption.com/ |
| File or email encryption | http://www.gpg4win.org/ |
| **FREE Bootable Anti-Virus Rescue CDs** | |
| Microsoft System Sweeper | https://connect.microsoft.com/systemsweeper |
| AVIRA Rescue | http://www.avira.com/en/support-download-avira-antivir-rescue-system |

| | |
|---|---|
| System | |
| AVG Rescue CD | http://www.avg.com/ww-en/avg-rescue-cd |
| F-Secure Rescue CD | http://www.f-secure.com/en_EMEA-Labs/security-threats/tools/rescue-cd/ |
| VIPER | http://live.sunbeltsoftware.com/ |
| **Online Virus scan** | |
| ESET | http://www.eset.com/us/online-scanner |
| SOHPOS | http://www.f-secure.com/en_EMEA-Labs/security-threats/tools/online-scanner |
| **Web server security** | |
| CloudFlar | http://www.cloudflare.com/ |
| **Rescue Tools** | |
| Windows password reset | http://pogostick.net/~pnh/ntpasswd/ |
| System Rescue CD | http://www.sysresccd.org/ |
| Microsoft Safety Scanner | http://www.microsoft.com/security/scanner/en-us/default.aspx |
| Emsisoft Emergency kit | http://www.emsisoft.com/en/software/eek/ |
| Rootkit scanner | http://public.avast.com/~gmerek/aswMBR.htm |
| **Logging** | |
| Splunk | www.splunk.com |
| Cloud based logging service | http://www.loggly.com/ |
| **Privacy tools** | |
| VyprVPN | https://www.goldenfrog.com/vyprvpn/vpn-service-provider |
| **Mics** | |
| Anti-Phishing toolbar for Firefox | http://toolbar.netcraft.com/ |
| Mcafee SiteAdvisor, browser add-on for web rating | http://www.siteadvisor.com/ |
| Secure Password Generator | http://www.pctools.com/guides/password/<br>https://domaindiagnosis.com/password.php |
| Secure file deletion | http://www.fileshredder.org/ |
| Security Tips for online Social Networking | http://blog.zeltser.com/post/8503487922/11-social-networking-security-tips |
| | http://www.selectrealsecurity.com/malware-removal-guide |