وزارة الاتصالات وتكنولوجيا المعلومات
Ministry of Information and Communications Technology

Information Security Framework for School Networks

The Ministry of Information and Communications Technology

Document Reference: ISGSN2012-10-01-Ver 1.0

Published Date: March 2014

Table of Contents

Definitions

In the application of these Guidelines, the following terms and expressions shall have the meanings assigned to each of them unless the context requires otherwise:

- **Computer Viruses –** attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files or devices on a system or through multiple systems in a network, that may result in the destruction of data or the erosion of system performance.
- **Information –** all information in the custody or under the control of the School, whether in electronic or other recorded format, and includes administrative, financial, personal and student information, and information about those who interact or communicate with the School.
- **Information Availablity –** the ability to access information or resources in a specified location.
- **Information Confidentiality –** ensuring that information is accessible only to those authorized to have access and is protected throughout its lifecycle.
- **Information Integrity –** the accuracy, consistency and reliability of the information content.
- **Misuse –** the use of information assets for other than the authorized purposes by either internal or external users.
- **Penetration –** attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs.
- **Personal data –** private, personal or confidential information, whether in electronic or written form, about identifiable students, families, employees, members of the public or any other persons.
- **Personal information –** recorded information about an identifiable individual.

- **Security –** the ability to protect the integrity, availability, and confidentiality of information held by a School and to protect network assets from unauthorized use or modification and from accidental or intentional damage or destruction. It includes the security of network facilities and off-site data storage; computing, telecommunications, and applications related services and Internet-related applications and connectivity.

1. Legal Mandate

Articles (4) and (5) of Decree Law No. (36) of 2004 establishing the Supreme Council of Information and Communication Technology (ictQATAR) acknowledges it as the highest competent authority in the communications and information technology affairs. ictQATAR has the authority and competence necessary for the discharge of such affairs and in particular the authority to regulate and to make policies for the two sectors of Communication and Information Technology in the State of Qatar.

2. Introduction

Schools across the world are vulnerable to cyber attacks, putting data of students, employees and administration at risk. This is very alarming, considering that it is currently a common practice for Schools to have personal and confidential information about students, parents and staff on School computers, personal laptops, home computers, USB memory sticks and other media. Schools have a duty to safeguard staff and student's personal data stored and transmitted electronically. These guidelines are provided to help Schools tighten up their practices and procedures for ensuring the security of that data.

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

The underlying principle of the guidance is that Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature by protecting its confidentiality, integrity and availability.

Why information Security

1. Ensuring Confidentiality of Information.
2. Ensuring Accuracy of Information.
3. Ensuring Availability of Information.
4. Improving productivity by ensuring network uptime and quick recovery from security breaches.

3. Scope and Application

This Information Security Guidelines document summarizes what is expected of all School staff in the course of their duties in relation to information security and computer equipment.
Its aim is to protect:

- Staff, students, parents and visitors;
- Assets, including information assets;
- School Records (administrative, financial, health, etc) ;
- School image and public reputation.

By reducing the risk of:

- Accidental loss or damage to assets;
- Unauthorized or unintended modification or disclosure of personal and/or confidential information or other misuses;
- Breach of information or any deliberate and harmful acts carried out through lack of awareness of their consequences.

By reaching the Goals of:

- **Prevention –** the better the prevention policies, the lower the likelihood of a successful attack occurring;
- **Detection –** detection activities should be ongoing and part of information security policies and procedures;
- **Response –** strategies and techniques to deal with an attack or loss and a plan to respond, restore operation, and neutralize the threat.

It applies to:

- All services in the School;
- All employees and students of the School;
- Any third person working for the School or on School premises.

This document provides the necessary information that enables staff and others meet their general responsibility to safeguard the School's information and assets. Schools may adapt the document to reflect their own circumstances in order to publish their own Information Security document.

4. Guidelines Articles

These Guidelines are meant to keep the data safe and the business running smoothly. The security guidelines consists of various rules and behaviors, 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.

4.1. Personnel Security

4.1.1. General responsibility and understanding of information security must be included in the induction procedures for all staff.

4.1.2. External contractors, consultants, trainers, temporary teachers/interim faculty and others employed on School premises or given access to School systems must be subject to checks and agreements appropriate to the services to be provided.

4.1.3. Work placements, students, volunteers, parents, and any other persons not subject to a contract of employment, and having access to School computer systems, including remote access, must be subject to confidentiality and security agreements

4.1.4. Temporary staff working in the School should not be provided with log-ins to systems which allows them access to sensitive data. Furthermore, paper records should be treated with the same caution sharing only the required amount of data for them to do their jobs effectively.

4.1.5. A record must be made of equipment, smartcards, etc, issued to new employees and anyone else listed in paragraphs 4.1.3 and 4.1.4.

4.1.6. On termination of employment, all School property must be returned or accounted for. Email, School network, library accounts and other system access must be cancelled. Passwords protecting sensitive data must be changed.

4.2. Information Security

4.2.1. Information is an important School asset and it must not be considered as a common resource to be freely exchanged.

4.2.2. Schools should develop and implement Information Security Awareness program to ensure that all personnel accessing or handling data are aware of their information security responsibilities.

4.2.3. All information, whether disclosable or not, must be protected from accidental and malicious loss or damage. Personal and confidential information must be protected from unauthorized and unintended access and disclosure.

4.2.4. Every personal dataset routinely shared with an external agency must be the subject of a sharing agreement.

4.2.5. The School should hold a central register of all data-sharing agreements and ensure that relevant staff are aware of the existence of any such agreements, and of their terms and scope.

4.2.6. The purpose and uses of collecting personal data must be limited to obtaining information that is relevant to the purpose. Such information should be disclosed with the consent of the individual concerned and/or the guardian. Such data should not be used for any other purpose, unless otherwise specified. Personal data may be disclosed only to persons who have the right to it. Personal data should not be accessed or viewed without legitimate reason.

4.2.7. Personal data should only be stored on secured network drives, secure PCs and laptops or in a secure on-line system or a Learning Platform, which require user authentication (login name and password) to access the data.

4.2.8. All personal data stored electronically should be systematically backed up as part of normal network management. Secure storage of these backups is essential and tests should be conducted regularly.

4.2.9. Schools must keep a secure record of all passwords used to encrypt sensitive data so that data can be recovered and changed if a member of staff leaves.

4.2.10. Schools should have a secure method for resetting passwords.

4.2.11. Personal data or any other confidential data transferred to a portable device should be encrypted and must be removed before the device is made available to another person in accordance with Qatar National Information Assurance Policy NIA.

4.2.12. In default configuration Email and Fax are insecure media for transmitting personal and confidential information and should be avoided where an alternative exists. The sender is always responsible for ensuring that the intended recipient of a confidential Fax is notified before it is sent.

4.2.13. In the exceptional circumstances where personal data has to be shared by email, the data must be sent as securely as possible for example by encrypting the attached data file using a strong password shared verbally.

4.2.14. Documents containing personal or confidential information must be disposed of by shredding. Paper containing personal data must not be re-cycled or used as scrap.

4.2.15. Documents, media, unneeded PCs and similar equipment for disposal should be stored securely until removed for disposal. All ICT equipment should be disposed of in accordance with Qatar National Information Assurance Policy NIA.

4.2.16. When working with personal and confidential data computer screens and keyboards should be positioned where they are not visible from outside the immediate work area.

4.2.17. Where a shared admin/curriculum network is in place, the School should have very clear procedures, understood and followed by all staff, to ensure the protection of the network.

4.2.18. Work at home must be carried out at a similar security level as office-based work. All staff working off the School site or at home must be aware of the additional and significant risks of :

a. information 'leakage' through being overlooked or overheard
b. the opportunity for hacking presented by Bluetooth or Wi-Fi
c. Leaving sensitive School data accessible on home computer systems.

4.2.19. The same precautions should be taken when accessing online confidential data at home and such data should not be copied on to the PC.

4.2.20. Anyone transferring personal data from School sources to their own personal computer or memory stick is personally liable for the security and breach? of that data and for any legal consequences.

4.2.21. When a staff member has access to a School laptop for personal use, the laptop should be set up with two different user accounts for School and personal use.

4.2.22. Staff should be aware of the data risk from viruses and Spyware from personal downloads and take strict precautions to prevent or eradicate such attacks. These issues should be covered in the School's Acceptable Use Policy for staff using electronic equipment.

4.2.23. Any staff member becoming aware of an incident that could compromise data security should report it to School management. Such incidents include, but are not limited to :

a. Unauthorized access or attempted access to computer systems
b. Unauthorized access to personal data in any medium
c. Accidental loss or disclosure of personal data

4.3. Hardware Security

4.3.1. Every user of the School network and stand alone computers should have their own user name, password and a set of rights appropriate to their work.

4.3.2. Access to all computer applications involving personal data must be controlled and protected by secure passwords

4.3.3. No external party, supplier, technician, bureau or other agency should be given access, either in School or remotely, to systems, data, hardware or networks unless an appropriate access agreement is in place to ensure they understand their responsibilities.

4.3.4. Staff user passwords, such as those for logging on to the network or School systems, provide an accountability trail and they:

a. Must not be recorded or shared with any other person or saved by the computer
b. Must be strong passwords (Long passphrase)
c. Must not consist of dictionary words, personal names or words that have associations with individual users
d. Must be changed regularly
e. Should not be minor variants of old passwords

4.3.5. Staff should take care to ensure that ICT equipments are protected against theft. All equipment should be physically secured where possible. Equal care should be given to protect equipments taken off site or home.

4.3.6. Schools should have procedures in place to ensure that all PCs and laptops, including those not connected to the School network, are regularly backed up and have up to date anti-virus, anti-spyware and security updates installed.

4.3.7. To avoid the risk of virus infection, emails that are obvious spam or with unsolicited or unexpected attachments should not be opened.

4.3.8. Software should only be installed on a School computer in accordance with the School's policy (which will cover issues such as licensing, open source, use at home, inventory, etc).

4.3.9. Hardware (such as Bluetooth and Wi-Fi adapters and personal laptops) should only be installed or attached to the School's network in accordance with the School policy due to the risk from hacking and virus infection.

4.3.10. If a virus is suspected then technical advice should be sought immediately.

5. References

SANS Reading
http://www.sans.org/reading_room/whitepapers/bestprac/securing-network-k-12-public-School-environment_1292

School eSafety Policy - Kirklees
www.**kirklees**safeguardingchildren.co.uk

YHGfL Guidance for creating an eSafety Policy
https://public.rgfl.org/esafety/Shared%20Documents/YHGfL_Guidance_for_Creating_a_School_eSafety_Policy.pdf

Broward County Public Schools
District Information Security Guidelines
http://www.broward.k12.fl.us/Ets_Web/tpp/policies.htm

The Arkansas Department of Education IS policy
www.arkedu.state.ar.us/commemos/attachments/IT_**Security_Policies**.doc

The Mississippi Department of Education
http://www.mde.k12.ms.us/docs/management-information-systems-library/enterprise_k12networksecuritypolicy.pdf?sfvrsn=2

Governemnt (Qatar) Information Assurance Policy
http://www.ictqatar.qa/en/documents/document/government-information-assurance-policy