Ras Al Khaimah American Academy				
Subject: Technical Security Policy			**SOP No:** RAKAA-IT-07	**Controlled Copy No: 1**
			Revision No: New	
Written by:	**ICT Manager** Asma Odawa	**Date:** May 22, 2022	**Based on:** Current practice	
Checked by:			**Supersedes:** New	**Issued on:** May 22, 2022
Approved by:	**Principal** Sandra Zaher	**Date:** May 22, 2022	**Distributed to:** Principal (Original)	**Pages:** 7
Authorized by:	**Principal** Sandra Zaher	**Date:** May 22, 2022	**Effective as of:** May 22, 2022	
			Review date:	

Contents

Introduction:

RAKAA School is doing everything possible to ensure the security of the school's infrastructure and network. We also ensure that:

- Only authorized staff has access to the data
- Each department will have access only to their files
- Logs of users access are recorded
- Monthly reviews and audits are performed by the ICT department to ensure the security of our school systems

Policy Statement

The security of the network and infrastructure is critical to the smooth running of operations. This policy supports secure network systems, processes, and procedures, as well as the protection of all confidential data on school servers, computers, and networks. It also supports efforts to reduce threats to the school, its students, or its staff. In addition, it ensures the system sustainability and continuity.

- ICT Managers are responsible for the management of the technical security and services
- ICT Managers are responsible for ensuring that software license records are up to date, and that regular checks are performed.
- The IT Department monitors and records user activity and reminds users of the Acceptable Use Agreement. Also IT department keeps up to date logs for the different systems and applications
- Reporting procedures for technical incidents is clear to all users and is included in the reporting policy
- As mentioned in the AUP users are not allowed to download exe files. ICT department is regularly testing the updates applied in the listing of applications and websites in the filtering system by connecting to different WLAN to confirm the same.

- Staff are not permitted to copy sensitive or restricted personal data from the school unless the data is encrypted, and password protected. This is for work related matters only.
- UPSs are connected to Servers, switches, Firewall, NVRs, amplifiers, and controllers to support the additional capacity and protect devices from power interruption and spikes
- Solar Winds system is used for monitoring the network performance

Network Security

- All networked devices including, servers, switches, firewall, backup systems, NVRs, UPSs, etc.. are in server room and IDF rooms. Access to server rooms and IDF rooms is restricted to authorized staff through appropriate access control. Fingerprint authentication is used to enforce access control, only IT and few staff members from the quality assurance department are granted access to perform their job functions.
- Users will be held accountable for securing their username and password. They must not allow other users to access the systems using their log in information and must immediately report any suspicion of a security breach.
- Desktop remote access is enabled for the support and installation of software and updates. This is managed only by the IT department
- Guests/visitors are not allowed to connect to local area network or Wi-Fi. In case they need to make product demos there is a school system that can be used in the conference room
- RAKAA ensure that staff and students networks are separated from main school computer networks, and utilize security policies to ensure the integrity of those computer networks
- Management, HR, IT and Accounts information are considered sensitive therefore we have created separate drives for each department to save their data in the file server. The access is shared only with authorized staff through the school's network. Important documents are protected with passwords

Antivirus/Antimalware

Antivirus software is a data security application placed in a computer system to guard against viruses, spyware, malware, Trojans, phishing attacks, spam assaults, and other online cyber threats.

Trend Micro Apex One Antivirus program is used in RAKAA to protect school servers, desktops, laptops, and devices connected to the school network from threats. IT department is always ensuring that all school devices have the antivirus installed and ensuring that is it always updated. In addition, logs are regularly monitored.

No user in school can quite or uninstall the antivirus from the system. Only the IT department has this kind of access.

Password Security

The school is responsible for ensuring that the infrastructure and network are as safe and secure as possible. A safe username/password is essential to safeguard the school system and to ensure that only authorized users can access the school data. Passwords are the frontline protection for the users' accounts and school information system. Therefore, users must comply and refer to this policy to safeguard their data by securing the privacy of their passwords.

- All school platforms, devices, networks, and systems will be protected by secure passwords that are changed on a regular basis. According to the details outlined in the Password Policy and Guidelines
- A copy of the Administrator passwords is kept with the Quality Assurance Manager
- Passwords shouldn't be displayed while being entered in the systems.

Filtering:

Content filtering allows RAKAA to prevent staff and students from accessing harmful and malicious content and websites while still providing them with good, appropriate, and pertinent information.

IT department is responsible for managing the web filtering and sometimes an external supplier is contacted for applying some upgrades in the system. External suppliers are given limited access until the service they were contracted for was completed and after that access will be denied for them.

RAKAA has Sophos firewall and filtration appliance which does the following:

- ✓ Secure data
- ✓ Filter online content
- ✓ Protect school's network and end users from the latest threats while accelerating cloud application traffic
- ✓ Maintain firewall log data with reporting tools that enable IT department to analyze network over time

Refer to the Filtering Policy for more information.

Monitoring

To achieve the aims of ensuring the safety of students and staff while they are in school and/or engaged in an online activity, Ras Al Khaimah Academy (RAKAA) ensures to provide education in the use of technology and create mechanism for monitoring system to identify, prevent and intervene when untoward incident happens. (Refer to the Monitoring Policy)

The ICT Managers are responsible for:

- Doing regular monitoring and filtering of the school IT system to limit the incident risk of illegal activities and inappropriate behavior.
- Making sure that the AUP is age appropriate and clearly understood by various groups of users.
- Implementing filter rules to prevent access to sites likely to contain harmful and/or illegal material.
- Ensuring monitoring software/systems are implemented and updated
- Reviewing system implementation and creating plans for improving the monitoring system

Backup Strategy:

- Data in school's management system Mograsys
  - The system provider is doing the backup
  - Also, they are sharing monthly backup for the database with the IT department.
  - IT department is doing monthly physical backup for the database in an external drive which is stored in the principal's house.
- Website
  - Hosting plan include automatic backup
  - IT department then download a copy of the backup monthly and store it physically in the external drive which is stored in the principal's house.
- Files in the network drives
  - Data stored by network users are backed up in file server and QNAP storage.
  - Also, a backup for these documents is stored physically in an external drive which is stored in the principal's house.
- Servers
  - Full backup for the servers is stored in an external drive which is stored in the principal's house.

Backup schedules for the network files and the servers are set through veritas backup solution.

Principal signed on a form confirming that the hard drives have confidential data and that she will ensure that it should be kept in a safe place and will be used and collected when required.

Disaster Recovery Plan

In case of any natural disaster backup stored in the external drives off campus in the principals' house will be used to for systems and files recovery.

Removable Media

Policy Statement

There is a wide increase in the number of IT security threats originating from removable media which infect systems with malicious code and/or remove sensitive data.

Portable devices that can be used to copy, save, store, and/or move data from one system to another are commonly referred to as removable media. Media devices come in various forms that include, but are not limited to, USB drives, flash drives or cards, write CDs, memory cards and external hard drives.

While removable media is widely used for data storage and transport, some of the features that make them convenient to use also introduce security risks, owing in large part to the fact that they are typically unmanaged storage devices.

To help mitigate the risks associated with removable media devices, the IT department recommends that all staff and students implement several best practices as below:

- Do not use personally owned removable media devices in school systems.
- Do not utilize school-owned removable media devices on home computers.
- Never use unidentified removable media devices in ANY system.

Maintain personal systems with the most recent patches and anti-virus signatures. Compliance with this policy, as well as the implementation of other mitigating measures, is critical to the security of RAKAA's information and systems.

IT department disabled the connection of the USB storage devices.

References:

- Filtering Policy
- Reporting Policy
- Monitoring Policy
- Password Policy & Guidelines
- Data Protection Policy
- Online Safety Policy