Cedarwood School

113 - 117 Dunmaglass Road, Glenferness

Prep Switchboard: 011 465 9830
Emergency: 071 609 7253

College Switchboard: 011 467 4889
Emergency: 072 617 5291

www.cedarwoodschool.co.za

Cedarwood School
IT Cyber Security Policy

This policy must be read in conjunction with the POPIA Manual

1. Introduction

The purpose of this policy is to highlight to the Pupils and all staff of the potential risks of cyberattacks for the school, making clear what we currently have in place to prevent such events occurring, and to highlight what is regarded as the basic principles of good cyber security.

A cyber-attack is an attack launched from one or more computers against another computer or network of computers. It can maliciously deactivate computers, steal data, or use a compromised computer as a launch point to further aggravate the attack. The two aims of cyber-attacks are to either disable the system or gain illegal access to the target computer or network. A cyberattack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation. Usually the attacker seeks some type of benefit from disrupting the victim's network.

While cybersecurity prevention measures differ for each type of attack, good security practices and basic IT hygiene are generally good at mitigating these attacks.

In addition to implementing good cybersecurity practices, we are advised to keep systems and security software up to date, leverage firewalls and threat management tools and solutions, install antivirus software across systems, control access and user privileges, backup systems often, and proactively watch for breached systems.

2. Common Types of Cybersecurity Attacks affecting schools

Here are some of the most common types of cyber-attack methods used by cybercriminal gangs around the world.

Phishing

Phishing is a technique used to deceive a target into taking harmful action such as downloading malware disguised as an important document. A targeted phishing attack could be used to gain access to a user's account that has important information (such as a member of the Senior Managment Team) or a user with administrative privileges to the network.

Phishing is usually in the form of an email sent to either a list of users or targeted at single user. The attacker would craft an email and disguise it to be seemingly normal, with malware attached that looks like it could be a normal document. The email could also include a link

that goes to a website designed to look like a familiar website and trick the user into entering their credentials.

To prevent phishing attacks, it is recommended the email system should have an effective filter, implementing email authentication methods like SPF, DKIM, and DMARC to filter potential spam. Users should also be trained on how to identify potential spam emails before clicking on any links or documents attached.

Ransomware

Ransomware encrypts the target files on the system so the user cannot access them. The attacker then demands payment to restore access to the files. A ransomware attack usually happens when a user opens a malware file or link on a network connected computer. The malware file has specific scripts to identify and encrypt the files in the target area.

Ransomware could be used to encrypt a school's financial and contact data so that the school would not be able to access it. To prevent ransomware attacks, it is a good practice to have On-access scanning enabled on all user devices to scan for viruses before accessing files. Firewalls should be enabled on host devices and anti-virus software should be updated with the latest security patches.

Password attack

Password attack is an attempt to gain access to systems by cracking the user's password. Once the user password is cracked, the attacker can gain access to either confidential data or an administrative account allowing access to all data or make significant changes to the network.

A targeted password attack usually involves the attacker finding out details about the user and then attempting to use that information to determine the correct password. Passwords are also sold on the dark web by criminal gangs that have been leaked or hacked from organisations. A good practice to follow is not using the same password twice.

Brute force

Brute force is an attempt to gain access to systems by trying different passwords to eventually guess the correct one. Similar to a password attack, the attacker could gain access to privileged user accounts.

Malware that is installed on the network with direct access to a systems login screen can be used to secretly attempt to guess a user's password.

One of the prevention tactics is to configure locking the accounts. Accounts should lockout if there are too many failed attempts at logging in. Audit logs should also be configured and regularly reviewed by the system administrator for any abnormal use of accounts.
Denial of Service (DDoS)

Firewalls

iShield
iShield Filtering protects our organization by blocking access to malicious, hacked, or inappropriate websites. Web filtering is the first line of defense against web-based attacks. Malicious or hacked websites, a primary vector for initiating attacks, trigger downloads of malware, spyware, or risky content.

Emails

MO 365 is used for all our emails. MO 365 email is encrypted using Transport Layer Security (TLS). This is a protocol that securely encrypts and delivers inbound and outbound mail while disabling eavesdropping between mail servers. Most major email providers use TLS but it is important to keep in mind that both the sender and receiver must use a TLS supported mail server to encrypt messages. Reports can be generated to identify how many messages were encrypted using TLS.

The school has a RM Disk-to-disk-to-cloud (D2D2C) Backup solution with a Cloudways backup server. This solution ensures we have an offsite backup of the school data.

3. National Cyber Security – Practical Tips

The National Cyber Security Centre has issues practical tips for everyone working in education. Each school needs to look after its data as well as manage the risks of using networked computers and servers.

Cyber security is about protecting the devices we use in school and the services we access on line, both at home and work, from theft or damage. It is also about preventing unauthorised access to the vast amounts of personal information we store on the devices and on line.

Cyber Security is important to schools because a number of schools have been seriously impacted by cyber incidents: perhaps a phishing attempt to steal money and passwords, or a ransomware attack that encrypts files preventing access. Many cyber incidents are untargeted and can affect any school that does not have basic levels of protection. As a school we hold lots of sensitive information, for example staff and parents bank details, medical information about students and safeguarding records. All of this must be kept safe and confidential.

RECORD OF CHANGES

Date	Page no, heading, brief description of changes	Entered by
10/11/2023	Policy created	Dorothy van Wyk