TECHNICAL INFORMATION SECURITY POLICY

July 2023-24

Passmores Co-operative Learning Community

Company no: 7736246

Technical Information Security Policy

Contents

1. Firewalling

1.1 Purpose

This is an internal policy that defines how Passmores Cooperative Learning Community (PCLC) manages firewalling technology and mechanisms for information technology systems used by its staff.

1.2 Responsibilities

Head Of Infrastructure is ultimately responsible for organisational compliance to this policy.

All users, inclusive of employees, subcontractors and suppliers with direct access to the PCLC's information technology systems are expected to conform to this policy.

PCLC's IT support team are responsible for providing support in complying with this policy.

Head Of Infrastructure is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated.

1.3 Default Credentials

PCLC always changes default credentials on network boundary firewalls. Default credentials are changed as a matter of priority upon receiving a new device, factory resetting a device, or commissioning a new service. Accounts and devices are never exposed to the internet before first having their default credentials changed.

1.4 Strong Passwords

PCLC follows the principles outlined in its Password Policy when changing network boundary firewall passwords.

1.5 Network Boundary Firewalls

PCLC requires that Network Boundary Firewalls have the following capabilities supported and enabled:

- HTTP and HTTPS proxy
- Gateway antivirus
- Multi-WAN with failover functionality (if multiple WANs are installed)
- Intrusion Prevention System

- Advanced Persistent Threat protection

1.6 Personal Firewalls (School Computers)

PCLC requires that the Windows host-based firewall is enabled on all network connected endpoints that have such ability.

1.7 Personal Firewalls (Home-based and Bring-your-own-device Computers)

PCLC requires that the Windows or Mac OS host-based firewall is enabled on all network connected endpoints that have such ability.

1.8 Blocked Services

PCLC does not allow services that are identified by the NCSC, GCHQ or the Cyber Essentials scheme as vulnerable to be allowed to connect through firewalls. Services that are identified as vulnerable are as follows:

- SMB
- TELNET
- NetBIOS
- tFTP
- RPC
- rLogin
- RSH
- rExec
- HTTP

1.9 Internet Access

Access to the internet from PCLC's Local Area Networks is granted only to devices that require access as an operational necessity. Restriction of access is implemented by a 'Blanket Deny'.

1.10 Maintaining the Register

PCLC maintains a register of all approved firewall rules permitted on Boundary Firewalls using the built-in access control list on the device, adding clear justification in the description of each rule. Rules are approved only by the Head Of Infrastructure.

2. Patch Management

2.1 Purpose

PCLC has a responsibility for ensuring the security requirements of its information assets are met. As defined in its information security policy, these requirements include confidentiality, integrity and availability. Malware that exploits software vulnerabilities presents the risk of breaching security requirements. Processes defined in this policy will reduce the risk of software vulnerabilities being exploited by malware threats. This internal policy applies to all physical and software assets listed in PCLC's information asset register.

2.2 Responsibilities

All employees with direct access to the PCLC information technology systems are expected to conform to this policy.

PCLC's IT support team are responsible for providing support in complying with this policy.

Head Of Infrastructure is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated.

2.3 Workstations

PCLC ensures that all its workstations are running an operating system that is actively supported by the vendor according to its development life cycle. Workstations running retired or legacy operating systems are removed from service. Automatic updates are enabled for all workstations' operating system, updating at the default frequency defined by the vendor.

2.4 Patching Schedule

PCLC aims to install all security patches within 14 days of release and aims to install patches not related to security within 90 days.

2.5 Problematic Patches

PCLC's IT support team will take all reasonable measures to ensure that updates known to be problematic are prevented from being installed until resolved by the vendor.

2.6 Software Licensing

PCLC does not operate unlicensed software and takes all reasonable measures to ensure that it meets all End User Licence Agreement terms.

2.7 Legacy Software

PCLC takes all reasonable measures to ensure that the software it uses is supported by its vendor. There may be occasions where no alternative software is available; in

this case the software must be approved by Head Of Infrastructure and marked as unsupported in the PCLC information asset register.

2.8 Monitoring and Internal Audit

PCLC conducts annual vulnerability scans to ensure compliance with this policy.

3. Ransomware

3.1 Purpose

This is an internal policy that defines how PCLC prepares to defend against the threat of ransomware attacks on the school's computer systems. The policy defines processes and procedures that aim to reduce the risk of exploitation by ransomware attacks, to lessen the impact and to quickly and safely recover from an incident.

3.2 Responsibilities

All employees with direct access to the PCLC information technology systems are expected to conform to this policy.

PCLC's IT support team are responsible for providing support in complying with this policy.

Head Of Infrastructure is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated.

3.3 Definition

The National Cyber Security Centre's (NCSC) definition reads: *"Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted."*

3.4 Preparation

PCLC recognises and acknowledges the threat of ransomware attacks and the severity of the impact on the PCLC's computer systems and operations and aims to prepare accordingly. To prepare for and defend against ransomware attacks, PCLC deploys strategies and controls which may include the following:

- **Data classification** - Not all data is equal and thus data should be classified and stored according to the sensitivity level. The school should be aware of the systems that process and store critical/sensitive data and such must be documented.

- **Effective backup strategies** - Backup systems are the first port of call in the case of a ransomware attack. Ransomware attacks aim to sabotage recovery operations thus, the school aims to implement effective backup strategies and data recovery operations by:
    - conducting regular backups of data, and most importantly, of critical/sensitive data
    - having offline backups preferably offsite
    - having multiple copies of the same file using different backup systems
    - scanning backup systems for malware where possible, especially before recovery
    - regularly testing data recovery operations
- **Staff awareness training** - The school conducts regular staff awareness training to educate staff in areas which include but not limited to best security practices, common attack vectors, phishing email attacks, password handling, reporting channels.
- **Patch management** – PCLC follows the patching schedule described in the PCLC's Patch Management Policy to reduce an attacker's probability of gaining access through a discovered security vulnerability.
- **Cyber insurance** - Cyber insurance will assist the PCLC with recovery costs in the case the trust suffers a breach.
- **Regular incident management plan rehearsal** - A timely and well-coordinated response to a ransomware attack might lessen the impact. PCLC aims to regularly review and test the incident management plan to ensure that it's up-to-date and that all the pre-defined roles and responsibilities are clearly defined.

3.5 Monitoring and Detection Controls

Network monitoring strategies and suspicious behaviour detection controls are implemented across the PCLC's computer systems and networks. This approach aims to implement technology best practices as well as non-technical approaches which may include:

- Ensuring anti-malware software applications are installed and enabled on all endpoints, virus signature databases are always up-to-date and files are set to be scanned on-access.
- Automated suspicious/unusual behaviour event notifications including the deploying a monitored 'honeypot' folder at the top of critical data directories that serves as an early-warning.
- Deploying robust email filtering systems to block, quarantine or flag suspicious emails.
- Reporting of suspicious emails or events by school staff.

3.6 Eradication and Recovery Process

In the case the PCLC is breached, the main aim is to contain the malware to prevent it from spreading to other systems. PCLC follows the NCSC guidelines to help limit the impact:

- Quick disconnection and isolation of infected computers, laptops or tablets from all network connections. If multiple devices are infected, network equipment including routers, switches and wireless access points may also need to be turned off.
- User credentials for user accounts associated with the infected device will be reset
- The latest patches will be applied to non-infected devices
- Infected devices are wiped and rebuilt
- All backup systems must be thoroughly scanned for malware before data recovery operations are commenced.
- Verify that endpoint anti-malware software applications are installed, up-to-date and enabled on all systems.
- Continuous monitoring of network traffic and anti-malware scans to verify if traces of the malware still exist.

3.7 Post Incident

Lessons learnt are discussed, documented and changes are made to the incident management plan and other internal processes where necessary.

3.8 Ransomware Payments

In the event that the PCLC's backup systems fail and data is unrecoverable, the only option might be to pay and that so being, PCLC follows the National Crime Agency (NCA) and the ESFA's guidance regarding ransomware payments.

4. Anti-Malware

4.1 Purpose

This is an internal policy that defines how PCLC protects its information assets from malware.

4.2 Responsibilities

All users, inclusive of employees, subcontractors and suppliers with direct access toPCLC's information technology systems are expected to comply with this policy.

PCLC's IT support team are responsible for providing support to PCLC in complying with this policy including managing and maintaining the anti-malware software solutions.

Head Of Infrastructure is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated.

4.3 Software Approval

PCLC prohibits any form of software that hasn't been approved and formally documented on its Approved Software Register.

4.4 Anti-Malware Software

All information technology assets of PCLC must have the organisation's designated anti-malware software installed where the software is compatible.

Designated Anti-Malware Software

PCLC has chosen Windows Defender as its designated anti-malware software solution.

Anti-Malware Software Configuration

PCLC's anti-malware software will be configured to perform:

- On-access scanning of files and web pages
- On-access scanning of removable media
- Scheduled full system scans on a daily basis
- Daily definition database updates

Home-based Staff and Bring-Your-Own-Device

PCLC requires all personal devices used by staff to access its information assets to have at least the operating system's default anti-malware software to be enabled and preferably its designated anti-malware software installed.

Anti-Malware Review

PCLC's IT support team is responsible for monitoring the installation and updating status of the anti-malware provision across the organisation.

This policy was reviewed and approved by the PCLC Finance, Audit & Risk Committee on 28th June 2023. It will be reviewed at least annually.