TCES THE COMPLETE EDUCATION SOLUTION

NATIONAL ONLINE SCHOOL

TCES IT Security Overview

CYBER ESSENTIALS

Cyber Essentials is a Government backed scheme that provides simple guidance to help us to protect our organisation, whatever its size, against a whole range of the most common cyber-attacks.

TCES is Cyber Essentials Certified as of the 6th of June 2022 and will have to recertify the 6th of June 2023.

Certificate number: IASME-CE-043128

BUILDINGS

TCES Schools and Head Office use FortiGate UTM Security which provides

- Web Filtering, network level
- Application Control
- Intrusion Prevention
- Data Loss Prevention

We have a segregated network with networks separating guest access.

DEVICES

Staff Device

All our windows devices are enrolled to Microsoft Intune for device management. All these devices have been configured using “Windows Security Baseline” and “Microsoft Defender for Endpoint security baseline”

We use Microsoft Intune and Desktop Central to deploy a set of technical policies to ensure the following is in place:

- Devices are encrypted with Bitlocker encryption XTS-AES 256bit
- Antimalware is installed and latest Antivirus signature updates are installed.
- Ensure all our devices are using the latest version of Windows OS
- Deploy company software – Office 365, Microsoft Edge Managed browser and Desktop Central

- All devices are remotely managed, this will enable us to Wipe, Retire the Device, Autopilot reset (reset the device to factory settings and apply all policies)

Pupils Devices

Google Cloud

TCES Pupils are provided with their own Chromebooks which is enrolled to Google's G-Suite which provides the following security measures.

- Chromebook security: Chromebooks use the principle of 'defence in depth' to provide multiple layers of protection, so if any one layer is bypassed, others are still in effect.
- Data Encryption
- Sandboxing
- Automatic Updates
- Verified boot
- Recovery mode

We block all applications turned on by default, prevent the installation of any software and we deploy and pin the following application to all our Chromebooks:

- Lexia Reading Core5 – Education
- OneDrive
- Word Online
- OneNote Online
- Sounds English: Learn to Read
- Lexia Power Up
- Microsoft Teams
- Netsweeper Client Filter

Netsweeper Client Filter / Impero WebChecker is a web filter at device level, meaning the web filter will work as long as there is an internet connection regardless of location.

Netsweeper is deployed to all pupils on the Pupil Organisational Unit

TCES deploys Impero: Webchecker to all Chromebooks to filter websites at all locations regardless of internet connection, the following categories are blocked:

Adult Mixed Content, Adware, Alcohol, Age Restriction, Bullying, Child Erotica, Child Sexual Abuse, Copyright Infringement, Criminal Skills, Directory, Extreme, Gambling, Games, Hacking. Hate Speech, Malformed URL, Malicious Web Obfuscation, Malware, Marijuana, Match Making, New

URL, Nudity, Occult, Open Mixed Content, Pay to Surf, Peer to Peer, Phishing, PIPCU, Pornography, Profanity, Remote Access Tools, Safe Search, Search Keywords, Self-Harm, Social Networking, Streaming Media, Substance Abuse, Terrorism, Tobacco, Viruses, Weapons, Web Chat, Web Email, Web Proxy

USERS

Staff Access Control

All our staff accounts are held in Microsoft Azure AD and are implemented with Conditional Access to access our devices and resources. Staff are required to use Multifactor authentication for further protection. In addition, the following measures are in place

- Require Multifactor authentication in all devices and resources
- Blocked non-UK sign ins
- Risky sign in policy
- Blocked legacy authentication

Pupils Access Control

We have a dedicated Microsoft Tenancy for our Pupils to login to their Chromebooks, we have set Policies to mitigate security risk such as data leakage with our main Microsoft (staff) Tenancy.

Further policies to our communication platforms “Microsoft Teams” are implemented:

- Disallow group chat
- Disallow adding or removing members from channels
- Disallowing teams’ reactions
- Disallowing to create / update / delete/ channels

Microsoft Public Cloud

Microsoft Public Cloud, also known as Microsoft Azure, offers a range of security features to help protect customer data and applications. Here are some of the key security features of Microsoft Public Cloud:

Compliance: Microsoft Azure is compliant with several industry standards, such as GDPR, HIPAA, and ISO, which ensures that customer data is protected and managed in accordance with regulatory requirements.

Encryption: Microsoft Azure uses encryption to protect data at rest and in transit. Azure also offers customers the ability to bring their own encryption keys to increase security and control.

Identity and access management: Azure provides robust identity and access management controls, including multi-factor authentication, single sign-on, and role-based access control.

Network security: Azure offers a variety of network security features, such as firewalls, virtual private networks, and distributed denial-of-service (DDoS) protection, to help protect against cyber-attacks.

Monitoring and logging: Azure provide customers with detailed logs and monitoring data to help detect and respond to security incidents.

Security Centre: Azure Security Centre provides customers with a centralized view of their security posture, as well as recommendations for improving security.

Threat intelligence: Azure uses machine learning and artificial intelligence to detect and respond to threats in real-time.

Overall, Microsoft Public Cloud offers a comprehensive set of security features and controls to help protect customer data and applications from cyber threats. Microsoft also has a dedicated team of security professionals that work to ensure the security of the platform and provide customers with support and guidance.

Google Public Cloud

Google Public Cloud, also known as Google Cloud Platform (GCP), offers a range of security features to help protect customer data and applications. Here are some of the key security features of Google Public Cloud:

Compliance: Google Cloud Platform is compliant with several industry standards, such as PCI DSS, HIPAA, and ISO, which ensures that customer data is protected and managed in accordance with regulatory requirements.

Encryption: Google Cloud Platform uses encryption to protect data at rest and in transit. Google also offers customers the ability to bring their own encryption keys to increase security and control.

Identity and access management: GCP provides robust identity and access management controls, including multi-factor authentication, single sign-on, and role-based access control.

Network security: GCP offers a variety of network security features, such as firewalls, virtual private networks, and distributed denial-of-service (DDoS) protection, to help protect against cyber-attacks.

Monitoring and logging: GCP provides customers with detailed logs and monitoring data to help detect and respond to security incidents.

Security Command Centre: Google Security Command Centre provides customers with a centralized view of their security posture, as well as recommendations for improving security.

Threat detection and response: GCP uses machine learning and artificial intelligence to detect and respond to threats in real-time.

Overall, Google Public Cloud offers a comprehensive set of security features and controls to help protect customer data and applications from cyber threats. Google also has a dedicated team of security professionals that work to ensure the security of the platform and provide customers with support and guidance.

FortiGate Firewalls

Fortigate is a popular network security platform developed by Fortinet, which provides a range of security solutions to help protect against various cyber threats. Here are some of the key security features of Fortigate:

Firewall: Fortigate offers advanced firewall capabilities, including intrusion prevention, application control, and web filtering to help prevent unauthorized access to the network.

Virtual Private Network (VPN): Fortigate provides secure VPN connections for remote access and site-to-site connectivity, using industry-standard encryption protocols.

Web Application Firewall (WAF): Fortigate offers a WAF to help protect web applications from common attacks, such as SQL injection and cross-site scripting (XSS).

Anti-malware: Fortigate provides anti-malware protection using signature-based and behaviour-based detection methods to identify and prevent malware infections.

Threat Intelligence: Fortigate uses threat intelligence to identify and respond to known threats and suspicious behaviour in real-time.

Multi-factor Authentication (MFA): Fortigate supports multi-factor authentication to help ensure secure access to the network.

Security Fabric: Fortigate offers a Security Fabric that integrates different security solutions and provides a unified view of the network security posture.

Overall, Fortigate provides a comprehensive set of security features and solutions that help protect against various cyber threats, such as malware, network intrusions, and web application attacks. Fortinet has a dedicated team of security professionals that work to ensure the security of their platform and provide customers with support and guidance.

ManageEngine Desktop Central

ManageEngine Desktop Central is a unified endpoint management solution that helps organizations manage and secure their IT assets, including desktops, laptops, servers, and mobile devices. Here are some of the key features of Desktop Central:

Patch Management: Desktop Central offers automated patch management to help keep all endpoints up to date with the latest security patches and software updates.

Software Deployment: Desktop Central provides software deployment capabilities to help streamline software distribution and updates across all endpoints.

Remote Control: Desktop Central offers remote control capabilities that allow IT administrators to access and troubleshoot endpoints remotely.

Inventory Management: Desktop Central provides inventory management capabilities to help IT administrators keep track of all endpoints, including hardware and software details.

Asset Management: Desktop Central offers asset management capabilities to help organizations manage and maintain their hardware and software assets.

Security Management: Desktop Central provides security management capabilities, including antivirus management, firewall management, and endpoint protection.

Mobile Device Management: Desktop Central offers mobile device management capabilities to help organizations manage and secure their mobile devices, including smartphones and tablets.

Overall, ManageEngine Desktop Central is a comprehensive endpoint management solution that offers a range of features and capabilities to help organizations manage and secure their IT assets. ManageEngine has a dedicated team of professionals that provide support and guidance to customers using their products.

Impero Web: Check

Impero Web: Check is a web filtering and monitoring solution designed for schools and educational institutions to help ensure students' online safety and compliance with acceptable use policies. Here are some of the key features of Impero Web: Check:

Web Filtering: Impero Web: Check provides web filtering capabilities to block access to inappropriate websites and content, based on predefined categories and custom filtering rules.

Monitoring: Impero Web: Check monitors internet usage in real-time, providing reports and alerts to help identify potentially harmful or suspicious online activities.

Compliance: Impero Web: Check helps schools comply with online safety legislation and policies, such as the UK's Prevent duty and the US's Children's Internet Protection Act (CIPA).

Customizable Policies: Impero Web: Check allows schools to customize filtering and monitoring policies to reflect their own acceptable use policies and safeguarding requirements.

Reporting: Impero Web: Check provides detailed reports on internet usage, allowing schools to identify trends, track user activity, and demonstrate compliance.

SafeSearch: Impero Web: Check provides safe search capabilities, which allow schools to block inappropriate search results from popular search engines, such as Google, Bing, and Yahoo.

Mobile Devices: Impero Web: Check provides web filtering and monitoring capabilities for mobile devices, including iOS and Android devices.

Overall, Impero Web: Check provides schools and educational institutions with a comprehensive web filtering and monitoring solution that helps ensure online safety, compliance, and safeguarding. Impero has a dedicated team of professionals that provide support and guidance to customers using their products.