Values
قيمي ترسم
هويتي

MARK VALUES AND QATARI VALUES
ARE AT THE HEART OF A DURHAM GIRL

IT Policy- ITP-05

IT Security and Access Control

Version 1.1 Aug 2024

First Implementation Date I October 2022
Review period I Annual
Date last reviewed I Aug 2024
Responsible person I ICT Director
Ratified by: School Leadership Team

Contents:

Introduction

Purpose

The purpose of this document is to provide direction and guidelines on IT Security and Access Control with Durham School. IT Security includes security of information across the organization, its access by internal and external parties, security applied on the network to protect information. Access Control includes access to the network, devices and applications on the network as well as external party access

Scope

This standard addresses the information stored on or transferred via computers, networks, telephones or other communication devices, as well as the usage and protection of the physical assets themselves

This document applies to all staff, contract labour, and any agents and representatives of DSGD(to the extent they exist) while acting on behalf of DSGD. It also applies to any other persons who, by formal agreement, are responsible for handling information that belongs to, or is under the control of DSGD*.*

Information Security

The Standards describes the high-level direction for information security management within DSGD and custodians of DSGD Information. It is based on three concepts: availability, integrity, and confidentiality:

- **Availability** ensures that DSGD Information is accessible when and where it is needed
- **Integrity** ensures that DSGD Information is correct or accurate to the degree anticipated by those who use it. It also ensures that DSGD Information has not been changed and has not been exposed to unauthorized modification, or disposal
- **Confidentiality** ensures that DSGD Information is not disclosed to anyone who is not authorized to access it. In support of this, is the idea of authorizing the sharing of DSGD Information on a need-to-know versus no-harm-knowing basis.
- DSGD and custodians of DSGD Information must be able to demonstrate that due diligence has been exercised in protecting DSGD Information and the DSGD environment. In this way DSGD can successfully protect its rights to its Information and the DSGD computing environment by, among

other actions, taking appropriate legal action including referring the matter to government authorities for civil or criminal prosecution. Illegal, unauthorized, or unethical disclosure, modification, misuse, or disposal of DSGD Information is prohibited.

Information about DSGD, its activities, its services, etc. is owned by DSGD, wherever it exists, regardless of location or storage medium (e.g., personally owned computing equipment, third party owned computing equipment, Cell Phones, etc.) DSGD Information exists in many forms, including but not limited to:

- audio
- diskette
- drawings
- electronic records
- facsimile of DSGD service and process (e.g., bill of materials, bill of process, contracts etc)
- optical disk
- paper or physical records
- photograph
- portable media (e.g., CD ROMs, Recorders, flash drives)
- slide or transparency
- video
- voice

General Information Security Standards:

- Information, in any form, relating to the business of DSGD and created or acquired using its resources, whether such information is owned or licensed by DSGD must be protected from unauthorized disclosure, malware, modification, misuse, and disposal, whether intentional or unintentional.

- All DSGD staff and users, custodians of DSGD Information, suppliers and alliance partners are individually and collectively responsible for protecting DSGD Information and the school's computing environment. They must comply with the Standards set forth in this document and any other information security standards created in support of this Standard.

- DSGD Information, when created or acquired, must be assessed according to its value and sensitivity to disclosure and managed according to need-to-know versus no-harm-knowing basis

- Any third-party information possessed by DSGD must be protected in accordance with the terms of any agreements with the third party

- Ongoing awareness and communications to inform DSGD staff and users of information security issues are mandated as part of the ongoing support of information security responsibilities and issues within DSGD

- DSGD Information must not be released to the public through media interviews, publications, seminars, conversations, disclosed in public forums, posted on the Internet, or in any other manner without a review procedure and/or management approval

- Suspicion or occurrence of any fraudulent activity, unauthorized disclosure, modification, misuse,

or disposal of DSGD Information, including intrusions or incidents of impaired or denied availability to the DSGD'S's computing and communications environment must be reported promptly to ICT Director

Information security on Computers:

All DSGD computers are password protected

All users are advised to store data important and sensitive data on only one-drive. Local storage locations are auto-synced to one-drive.

Users must employ all reasonable means to physically secure their laptops when not in use, including using locking devices where provided. Users need to secure their laptops in the workplace, at a residence, while travelling or when left in a vehicle.

All DSGD computers have restricted user privileges. System administrator privileges and/or the system administrator role are restricted to IT staff only.

Virus Protection

DSGD uses **Sophos Central Intercept X Advanced (Anti-ransomeware solution)**
The school subscribes to Sophos Central Intercept X Advanced End point Protect Anti-Virus software which provides virus protection across the school computers. Sophos has a management console on the cloud which reports regularly if any of the clients need updating, and also if there is a security threat on any of the devices.
Sophos Intercept X is the industry leading Endpoint Security solution that reduces the attack surface and prevents attacks from running. Combining anti-exploit, anti-ransomware, deep learning AI and control technology it stops attacks before they impact the systems.

Key highlights:

Stop Unknown Threats
Deep learning AI in Intercept X excels at detecting and blocking malware even when it hasn't been seen before. It does this by scrutinizing file attributes from hundreds of millions of samples to identify threats without the need for a signature.

Block Ransomware
Intercept X includes advanced anti-ransomware capabilities that detect and block the malicious encryption processes used in ransomware attacks. Files that have been encrypted will be rolled back to a safe state, minimizing any impact to business productivity.

Prevent Exploits
Anti-exploit technology stops the exploit techniques that attackers rely on to compromise devices, steal credentials and distribute malware. By stopping the techniques used throughout the attack chain Intercept X keeps your organization secure against file-less attacks and zero-day exploits.

Reduce the Attack Surface
Control which apps and devices can run in your environment, block malicious websites and potentially unwanted apps (PUAs) before they reach user or device.

Synchronized Security
Sophos solutions work better together. For example, Intercept X and Sophos Firewall will share data to automatically isolate compromised devices while cleanup is performed, then return network access when the threat is neutralized. All without the need for admin intervention.

Highlights
- Stops never seen before threats with deep learning AI
- Blocks ransomware and rolls back affected files to a safe state
- Prevents the exploit techniques used throughout the attack chain
- Reduces the attack surface with app, device and web control
- Performs threat hunting and IT ops security hygiene with XDR
- Provides 24/7/365 security delivered as a fully managed service
- Easy to deploy, configure and maintain even in remote working environments

Firewall

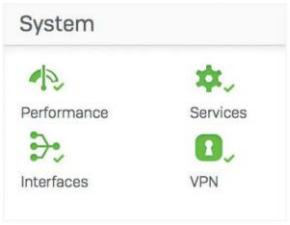
DSGD uses **Sophos XGS 3100** (Next Gen Firewall Appliance) with Sophos XGS Xstream Protection & Web Server Protection Subscription License. **Xstream Protection Includes:** Base License, Network Protection, Web Protection, Enhanced Support, Zero-Day Protection, Central Orchestration

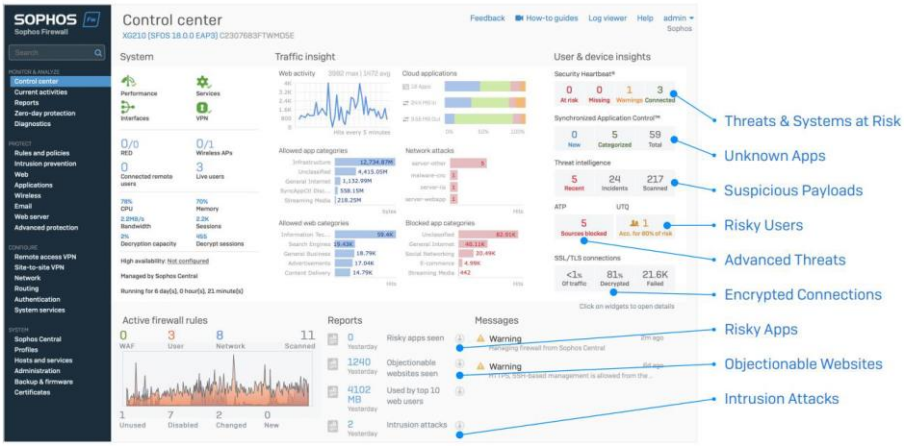
Control Center

Sophos Firewall's Control Center provides high level of visibility into activity, risks, and threats on our network.

It uses "traffic light" style indicators to focus our attention on what's most important.

If something's red, it requires immediate attention. Yellow indicates a potential problem. And if everything is green, no further action is required. Threats & Systems at Risk Risky Users Risky Apps Unknown Apps Advanced Threats Objectionable Websites Suspicious Payloads Encrypted Connections Intrusion Attacks Every widget on the Control Center offers additional information that is easily revealed simply by clicking that widget. The status of interfaces on the device can be obtained by clicking the "Interfaces" widget on the Control Center.





Internet access restrictions are applied via custom policies on the Firewall

Eg. Blocked all entertainment, weapons, movie, nudity, shopping, music, P2P clients, exe downloads, all social media except WhatsApp.

Blocked all gaming website categories.

YouTube allowed for authenticated users.

Exception rules are created on need-to-have basis.

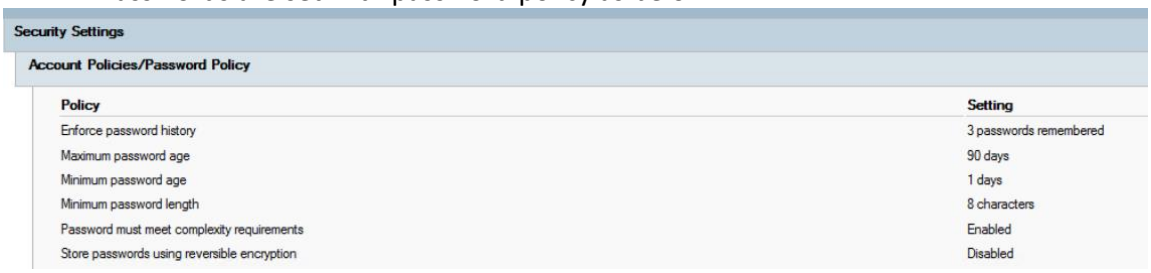
Patch Management

- All computers in the DSGD network are set to auto-update Microsoft applications and Windows as and when updates are released from Microsoft. The schedule of restart is configured to be taking place after office hours.
- Updates for major applications – Engage & HRMS systems are done by the application vendors as they are hosted on their cloud.
- Network devices patch management and upgrade is done by IT Maintenance contractor on their scheduled visits.

Access Control

All staff are provided with Microsoft accounts which they use single-sign-on for access to:

- Outlook email
- Team
- One-drive
- Business Central ERP (D365)
- HRMS System
- Passwords are set with password policy as below:



Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	3 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

- Local AD is synced with Azure AD.
- Engage application credentials are provided by the ICT support team

Active Directory Group Policy

AD Group policy is applied to staff and student computers to implement local restrictions on the network. Below is a brief overview of domain policy:

- Block download and installation of .exe files
- Block USB storage media, allow USB I/O eg. Mouse/KB
- Block changes to system settings, control panel
- Block access to Appstore
- Screen saver on after 5 minutes of inactivity
- Prevent access to the command prompt
- Prevent access to Registry editor
- Set password complexity and 8 digit minimum.

OU structure

Organizational

Units:

- DSGD Computers
    - Laptops
    - Desktops
    - Tablets
- DSGD Users
    - Admin Staff
    - Teaching Staff
    - Teaching Assistants
    - Students
    - IT Staff
- Servers

- Security Groups
    - DSGD All
    - IT
    - Finance
    - HR
    - Management
    - Teachers
    - Teaching Assistant