Technical Security

1. NETWORK SECURITY

- The network is protected with a Next generation FortiGate firewall (NGFW) which is optimized and configured with WAN Redundancy
- The network is securely divided into 4 Virtual LANS. Admins, Faculty, Student and Guest respectively.
- Each VLAN have unique security level and authentication to access the WAN and LAN
- The network is configured to identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in the network traffic
- The network configured to deliver industry's highest SSL inspection and packets deep inspection

NETWORK ACCESS REQUIRE USER AUTHENTICATION

	STAFF	STUDENT	PARENTS	GUEST
WIFI	√	√	√	√
PRINTER	√	*Not allowed*	*Not allowed*	*Not allowed*
STORAGE SERVER	√	√	*Not allowed*	*Not allowed*
CLOUD STORAGE	√	√	√	*Not allowed*
DESKTOP/LAPTOP	√	√	*Not allowed*	*Not allowed*
DOOR ACCESS CONTROL	√	*Not allowed*	*Not allowed*	*Not allowed*

2. PHYSICAL SECURITY OF DEVICES

2.1.0 DOOR ACCESS CONTROL SYSTEM

- All the main doors in the building are protected with RF ID Door access control system. The users can pass only though the permitted doors.
- The door access card will be disabled during vacation and long holidays
- During holidays entry to the campus requires supervisor/ managers approval
- In case of LOSS/ Damage the Access cards will be disabled immediately from IT Helpdesk

.

2.1.1 CCTV SURVEILLANCE

- All the areas of the campus is protected with CCTV surveillance camera's
- The cameras are 24/7 monitored by security guards on duty

- The camera visuals records are backed up in system at least for 30 days for review/Investigation
- The CCTV network is using separate VLAN network for extra security and intrusion prevention

2.2.2 SERVER ROOM/IT EQUIPMENT ROOM ACCESS

- Access to server rooms and IT equipment rooms are restricted to only those whose job responsibilities require that they maintain the equipment or infrastructure of the room.
- Signs are placed at the entrance to server rooms and IT equipment rooms, warning that access is restricted to authorized personnel and prohibiting food, drink, and smoking.
- Doors to server rooms and IT equipment rooms are fireproof and secured with locking system
- Server rooms and IT equipment rooms are monitored by IP cameras 24/7.
- Server rooms and IT equipment rooms have redundant power sources to run the systems in case of a power failure or outage.
- The server room equipped with cooling control system to protect the devices form the physical damage due to the heating

2.2.3 COMPUTERS AND LAPTOP

- All the computers in the CPS network are connected with school domain.
- Access to the computers (personal / computer lab) require unique password provided by CPS IT Helpdesk

2.2.4 WIRELESS NETWORK

- The network is divided into 4 VLAN for the better security and control over the LAN
- All the data traffic in the wireless network is protected with WPA2 Network encryption.
- Wireless devices are controlled by access controller and the IT admin keep the firmware up to date
- Daily monitoring will be carried out to find out the presence of rouge access points in the network

2.2.5 PRINTER

- All the multifunctional network printers are secured with authentication
- All the users will have unique user credentials for accessing the printer
- The printer will not process any un authorized print jobs

2.2.6 STORAGE

Local documents stored on local storage server or password protected desktop and laptop computers. This information's are backed up in Cloud storage so the documents and files can be restored in the event of a physical problem with the machine or if individual files or folders are inadvertently removed.

- A RAID 5 Storage backup is used for Storing and sharing the data locally. Data access permissions are controlled by IT Helpdesk with the Active- directory user policies
- The local storage server data is also keep a backup copy to an external storage device for data loss prevention.
- A copy of storage server data is automatically sync to the cloud server for the data redundancy and disaster recovery
- School faculty and staff and students only have access to a network drive provided by IT Helpdesk.
- Along with the local file server access Staff and students have access to the cloud storage.

- An internal audit conducted by the IT Team lead by the IT Administrator. The audit report is submitted to the online safety coordinator for review. Surprise audit may be conducted by the online safety leader/ coordinator to monitor the responsibilities of the IT Administrator

2.2.7 CLOUD STORAGE

For Student

- Each student gets 5gb cloud storage space in Microsoft servers to securely backup their data
- A dedicated storage server available for locally sharing the data within the computer lab . The Data stored in the storage servers are again backed up to the cloud servers automatically.

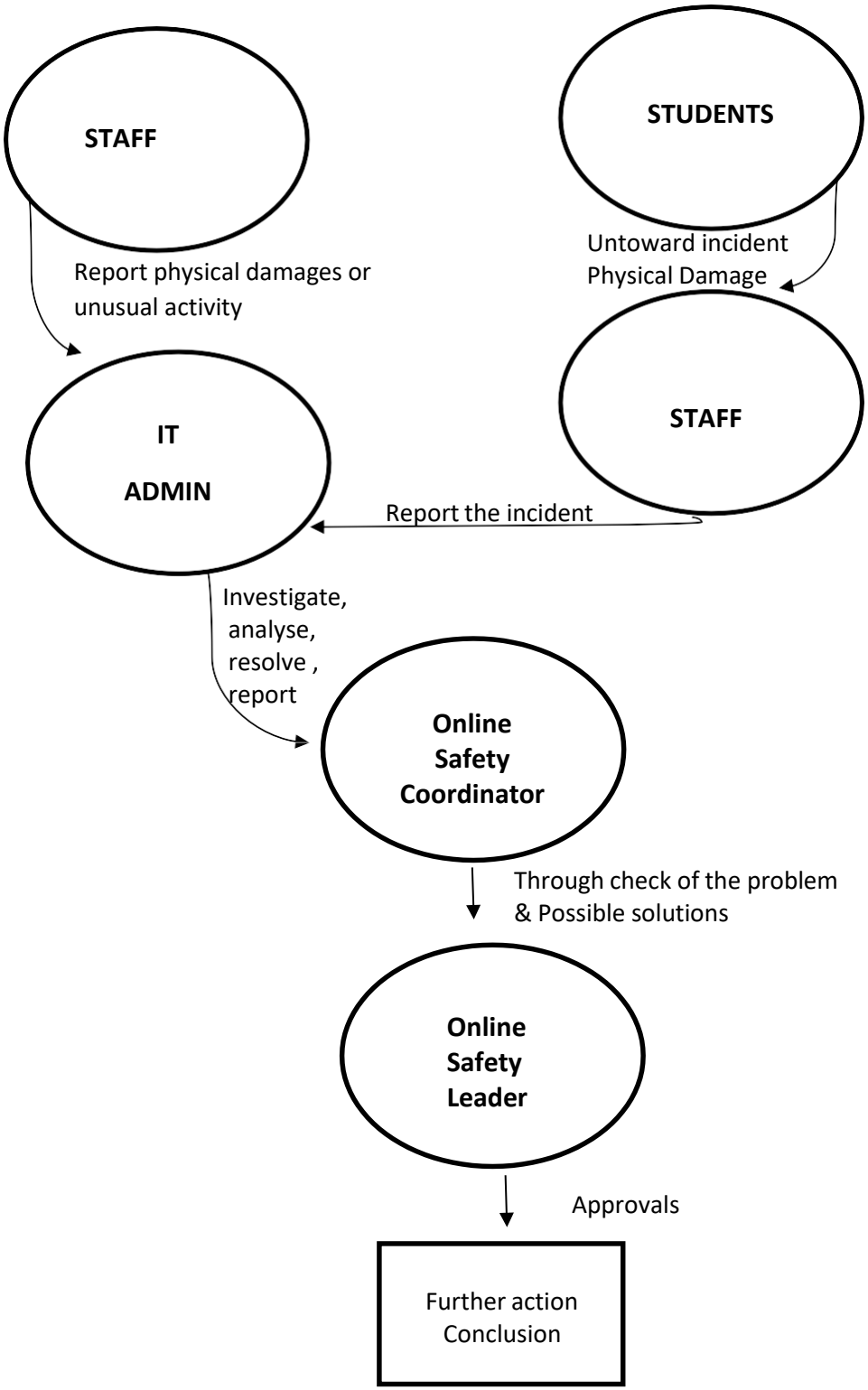
For Staff:

- All employees of Crown Private School have unlimited storage access to the google cloud service for backup the data. It is recommended that, the staff should back up their data daily or install an automatic backup (google cloud back up /sync) software in their system. For HR, Accounts officers, admission in charge and some admin users must install automatic cloud back up and sync software recommended by the IT Administrator
- A dedicated storage server available for the local sharing of data within the CPS Network. The Data stored in the storage servers are again backed up to the cloud servers automatically.
- Files may be copied re writable storage media (e.g., hard disks, and flash memory devices/thumb drives). These media must be stored in a secure location.

3. ANTIVIRUS/ MALWARE PROTECTION

- CPS network is secured with latest anti- virus definitions from the firewall
- End devices are secured with end point protection software
- All the computers attached to CPS network is secured with anti-virus software
- IT administrator regularly updates the additional patches to the antivirus application when necessary
- All students, staff wishing to use personally owned computers/mobile devices inside the CPS Network must have antivirus software installed before their system is given for the network access.
- Any virus-infected computer will be removed from the network and remain off the CPS network until it is verified as virus-free by CPS- IT Helpdesk
- All employees and students are responsible for taking reasonable measures to protect against virus infection/spread
- Employees /students must not attempt to either alter or disable anti-virus software installed on any computer attached to the CPS network without the express consent of the IT Administrator
- All the computers will be regularly checked for the malware/ adware infection and affected computes will be disconnected from the network with immediate effect and the system will be wiped with malware apps.
- Students and staff must avoid downloading freeware or untrusted contents from internet.

3.MONITORING / REPORTING BREACH OF TECHNICAL SECURITY



Prepared By	Reviewed By	Approved By
IT Administrator	Vice Principal	Principal
IT support coordinator	Online safety coordinator	Online safety Leader

IT UPGRADES

Academic Year 2021-22

SERVER REDUNDANCY

Currently we have a storage server and application server. The next IT upgradation is to create redundancy for this server for the server redundancy.

STORAGE UPGRADATION:

The current Raid 5 storage for storing shared file documents. An automatic back up and sync is added for back up the data to cloud

DATA PROTECTION

Dedicated Email Security and End point protection is activated

ANTIVIRUS AND MALWARE

Upgrade the current antivirus system to Endpoint Detection and Response for the comprehensive data collection and monitoring. Managed Endpoint Detection and Response uses artificial intelligence to stop advanced threats and malware at the most vulnerable points.

MANAGED SERVICE:

On site/ Off site backup and support assistance from the IT vendor for the maintenance of existing infrastructure and instant support for the hardware and software issues.

CCTV VIDEO WALL

Dedicated video wall for the security guard to monitor all the surveillance camera at the same instance without changing the screens

PHYSICAL SECURITY

Specialized locking system for server room entry , which allow the server room door entry with biometric recognition or with the card and pin code combination entry CCTV server room is locked with Card based acess control system

DOOR ACCESS CONTROL SYSTEM

Provisions are made to secure all the main doors access with NFC cards

ACCEPTABLE USE OF TECHNOLOGY

Acceptable use is always ethical, reflects academic honesty, shows restraint in the consumption of shared resources and protects all Information Technology (IT) Resources from any unauthorized or unintended use. It demonstrates respect on system security mechanisms, and. The establishment of this policy is to safeguard and protect the IT systems usage inside outside the school

In making acceptable use of technology resources users must:

1. Use technology only for authorized purposes;

2. Protect the ID card and system from unauthorized use. Users are responsible for all activities on their user ID or that originate from their system;

3. Access only files and data that are you own, or that are publicly available.

4. Use only legal versions of copyrighted software in compliance with vendor license Agreements

5. Be considerate in the use of shared resources. Refrain from overloading networks, with excessive data, or wasting computer time, disk space un necessarily

6. Use only authorized software unless approval is given by the IT Administrator to load other software;

In making acceptable use of technology users must NOT:

1. Use another person's system, files, or data without authorisation;

2. Use computer programs to decode passwords or access control information;

3. Engage in activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging or deleting files and directories;

4. Use school systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates;

5. Make or use illegal copies of copyrighted software, store such copies on school systems, or transmit them over school networks;
6. Use other employees id cards for printing

7. Use the school systems or networks for personal gain. For example, using school system or networks, for performing work for profit , in a manner not authorized by the school(crypto mining , etc)

9. Engage in any other activity that does not comply with the general principles presented above;

10. use computer lab facilities at the school unless enrolled as a current student, employed by the school or granted permission;
11. install personal equipment on school owned equipment without permission from the Online safety leader or online safety coordinator. These include printers, monitors, LCD displays, keyboards, access points, routers, IP phones web cams etc.

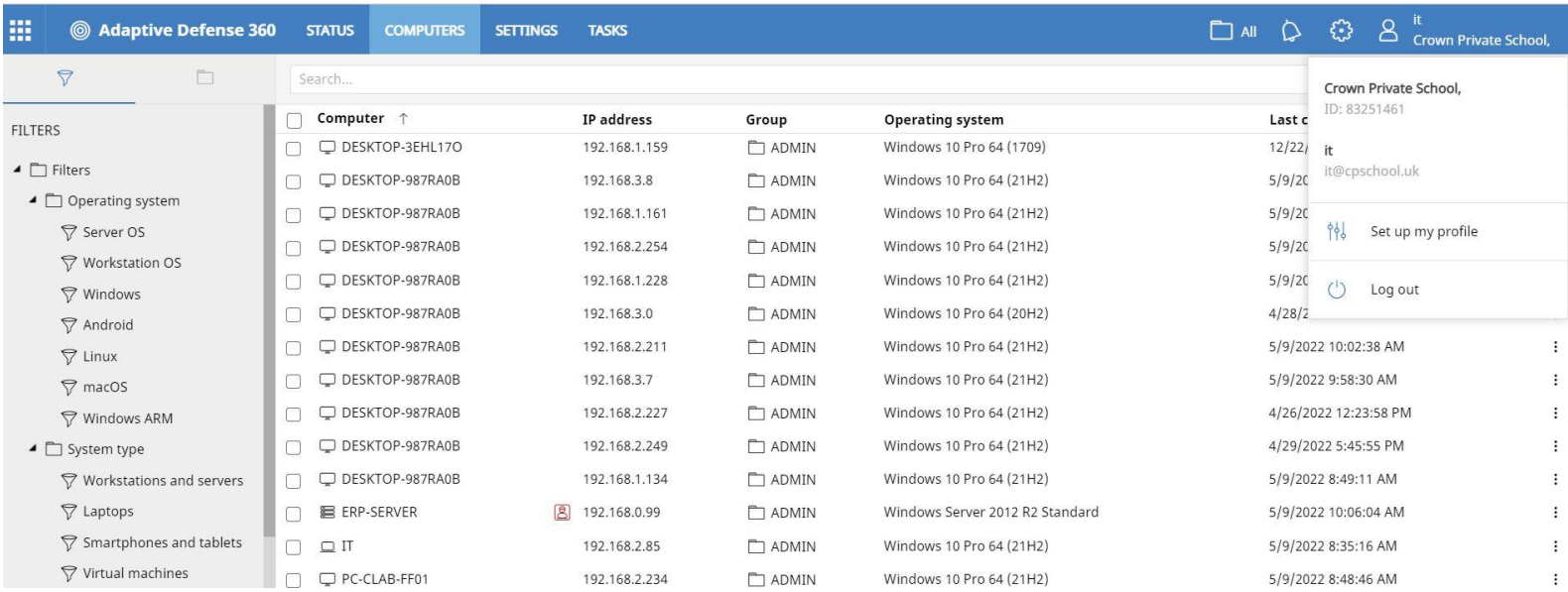
INTERNET GUIDELINES

1. Internet Access

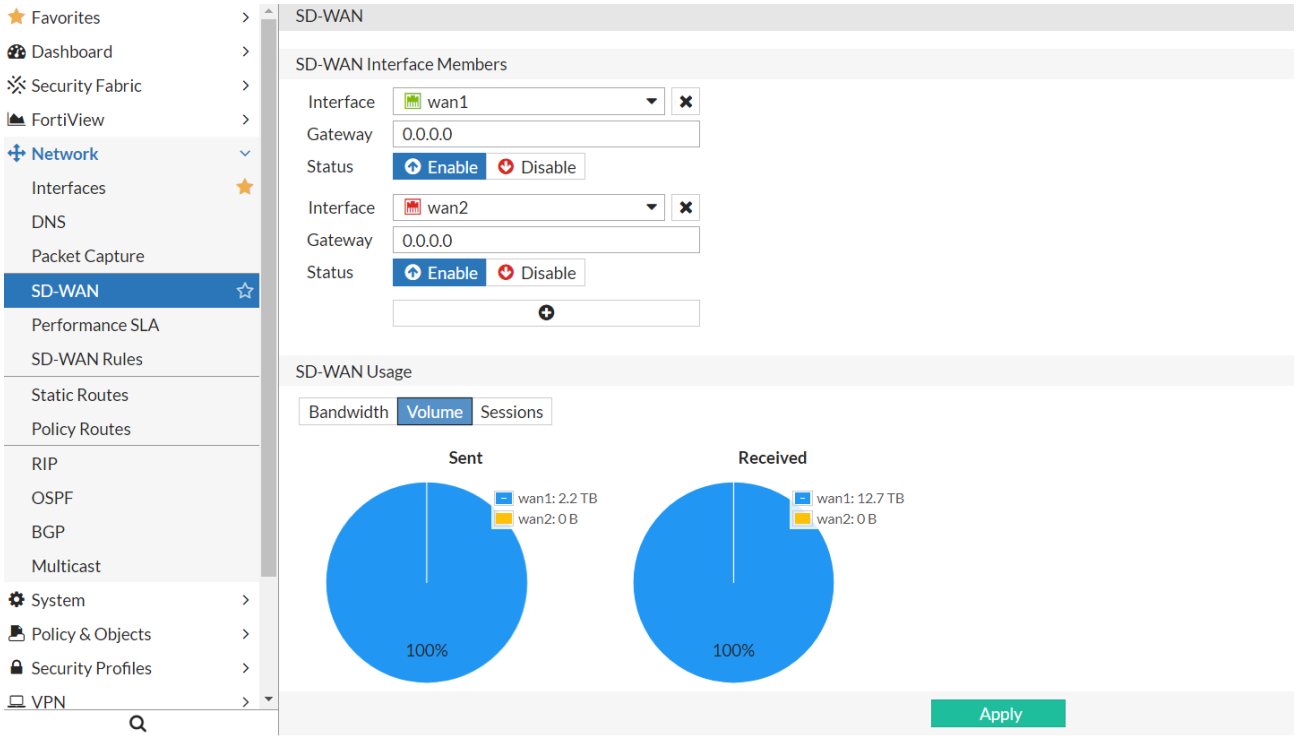
- Users must adhere to the following guidelines in addition to the general guidelines listed above:
- Access to the Internet should be used for purposes relative to classroom and work assignments and not for recreational purposes, including digital and social media;
- Access to the Internet may not be used for unethical, illegal, or criminal activities;
- Internet sped will be limited due to the number of people online and equipment
- Availability, so please do not use for heavy uploading /downloading activities during the school hours

- Downloading files from the Internet to the hard drives of lab PC's is prohibited;

MONITORING LOGS _END POINT PROTECTION



SD WAN – FOR INTERNET CONNECTION RESILIENCE



Threat Protection & Intrusion prevention