Risk Assessment

**Organisation:** Holmview Primary  
 **Version:** 1.0  
 **Effective:** n/a  
 **Owner:** Principal  
 **Review cycle:** Annual, and after any major change or incident

# Table of Contents

[Scope 2](#_Toc985657979)

[Definitions 3](#_Toc320921688)

[Risk Criteria 5](#_Toc1013333323)

[Threat Sources 5](#_Toc2104062575)

[Summary 6](#_Toc1712395858)

# Scope

The objective of Holmview Primary School is to provide a safe and secure environment for every student to learn and develop key skills and knowledge. In order to achieve this, any risks associated with the proposed school network must be identified and a plan must be made to mitigate, accept, transfer or avoid these risks.

The following points are what this risk assessment will cover:

* **People:** Students, staff, visitors, contractors, parents, volunteers and MSP’s.
* **Endpoints:** Student chromebooks and iPads, Staff laptops, classroom AV and mobile phones.
* **Networks:** WAN out to ISP, switching, WiFi (staff, student, etc.) and firewall(s).
* **Servers and Services:** Directory services and ldap, file sharing, printing, device management, email and CCTV servers.
* **Cloud and SaaS:** Online learning portals, parent portals, cloud hosted services, school management software and other software as a service.
* **Facilities and IoT:** Server rooms, CCTV cameras, door access, PA systems and printers.
* **Data:** Personal data of staff and students, student records, health records, financial data and assessment pieces.

This risk assessment is designed to comply with regulatory authorities and laws. Such as the Information Privacy Act, Child safety and duty of care and copyright and educational licensing as well as records retention.

# Definitions

These are definitions for terms used in this report and in the accompanying spreadsheet.

* **Risk:** The combination of the likelihood of an event occurring combined with the impact of the event occurring.
* **Asset:** Any object, property or intellectual property belonging to Holmview Primary School, including but not limited to: networking equipment, SSIDs, server rooms, mobile endpoints, etc.
* **Process:** The method or way in which something is carried out or done, such as creating or modifying user accounts.
* **Threat Event:** Any event or occurrence that has the potential to have an impact on Holmview Primary School.
* **Owner:** The person who is responsible for making sure that necessary treatment for an associated risk is carried out in a timely manner.

# Risk Criteria

The risk criteria and rankings can be found in the accompanying Risk Table spreadsheet. It measures the impact of an event in a scale of 1 to 5. The scale is as follows:

1. **Insignificant** (negligible impact, little or no impact to privacy or cost)
2. **Minor** (short outage or very little cost)
3. **Moderate** (Hours possibly days of limited disruption, small amounts of personal data compromised, moderate cost)
4. **Major** (Multiple hours, days or weeks of widespread outage, sensitive data exposed, mandatory notifications, large cost)
5. **Catastrophic** (Entire site closure for days or longer, Widespread sensitive data leaks, serious harm to people, extremely large cost to the school)

The likelihood of an event occurring is also measured on a scale of 1 to 5. An explanation of the different levels are as follows:

1. **Rare** (May occur under very specific exceptional circumstances)
2. **Unlikely** (This event could occur sometimes, once in a decade)
3. **Possible** (This event could happen or is known to happen, once a year)
4. **Likely** (This event can easily occur, once a month)
5. **Near Certain** (This event happens all the time, weekly or possibly daily)

# Threat Sources

There are various sources of threats which could potentially impact any of the previously mentioned scope. It is possible that there are multiple threat sources that could affect any of the previously mentioned items in the scope. The sources of these threats are as follows with some examples:

* **External:** Phishing, ransomware, terrorism, DDoS and SaaS being compromised.
* **Internal:** Misuse of accounts and devices, error in data handling, inappropriate privileges being given out.
* **Environmental:** Flood, Cyclone, Lightning, Rain, Power outages and hail.
* **Privacy and child safety:** Inappropriate content on the internet, malicious communications and mishandling of student information.
* **Technical:** Outdated software, insecure protocols being used, lack of sufficient monitoring and logging and weak configuration.

# Summary

As seen in group03-risk-assessment-table.xlsx there are many rules that Holmview primary school will face. However, when appropriate measures are taken, all these risks are taken down to a manageable level where residual risks can be accepted or instead passed on through insurance. Some key methods to reduce risk are multifactor authentication, strong filtering both inside and outside the network, regular monitoring and logging and backups. It is important to note that this table is not fully inclusive of all future risks that may arise and should be updated regularly with any changes. Any future changes where the residual risk score is higher than 10 must be either escalated or formally accepted by the school board with regular reviews.