Disaster Recovery & Backup Policy

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

# Table of Contents

[Table of Contents 1](#_Toc93464163)

[Purpose 1](#_Toc1352046929)

[Scope 2](#_Toc1344696877)

[Principles and Definitions 2](#_Toc1131586948)

[Recovery Targets 2](#_Toc1708248649)

[Backup Standards 3](#_Toc1684640503)

[Coverage 4](#_Toc1513889004)

[Frequency and Retention 4](#_Toc1039964698)

[Storage 4](#_Toc1329365168)

[Roles and Responsibilities 4](#_Toc511760255)

[Recovery Priority Order 5](#_Toc1844421130)

[Exemptions 5](#_Toc43841156)

[Review 5](#_Toc1672210855)

# Purpose

The purpose of this document is to ensure that in the event of a critical failure or some other disaster the school can protect, recover and resume normal operations. This policy defines the standard for backups and recovery as well as the roles, testing and gives a recovery plan.

# Scope

* **Systems:** On premise servers, networking, endpoints, databases, file storage, locally hosted applications as well as cloud hosted servers, applications and also SaaS.
* **Data:** The personal data of staff, students and parents. Such as student records, financial and payroll data, assessment pieces and also other files such as emails.
* **People:** Staff, external contractors, students and volunteers.

# Principles and Definitions

* **Immutable:** Written to once and then never modified, stored securely.
* **SaaS:** Software as a service.
* **Incremental:** An incremental backup is a backup that only backs up changes made to a system, e.g. it only copies new commands run.
* **3-2-1-1-0 Rule:** 3 copies, 2 media types, 1 off-site, 1 offline-immutable, 0 errors after verification.
* **Least Privilege & Separation of Powers:** Ensures that the integrity of backups can be maintained while being as secure as possible.
* **Restore-first mindset:** Backups are there to be restored quickly in the event of a failure and therefore are not just there to store data. This ensures that services resume as quickly as possible.
* **Privacy by design:** Backups are encrypted and stored securely. This ensures that access and retention is aligned with legal requirements for storing sensitive information.

# Recovery Targets

|  |  |
| --- | --- |
| Data set/service | Importance |
| Identity SSO | Critical |
| Email & communication | Critical |
| Parent portal | Medium |
| File sharing and Collaboration | Critical |
| Finance & Payroll | High |
| DHCP/DNS | High |
| Printing | Low |
| WiFi and Core Wired Network | Critical |
| Classroom AV | Medium |
| IOT Devices | Low |

# Backup Standards

## Coverage

* **On premise:** All servers/VMs, file shares, databases, hypervisor configuration, network devices (such as a firewall), images and mdm policies.
* **Cloud and SaaS:** Use a third-party backup for things such as google drive and Gmail as well as for any config for SaaS products.
* **Endpoints:** Critical data on staff and student devices.

## Frequency and Retention

* Daily incremental backups with weekly full backups for on premise data.
* Daily or hourly snapshots of logging for high priority data such as financial.
* Daily backups for SaaS as well as the capacity to restore individual items such as a file in google drive.
* **Retention**
  + Daily Backups: 30 days
  + Weekly Backups: 12 weeks
  + Monthly Backups: 1 year
  + Yearly Backups: 7 years to ensure compliance

## Storage

* **Media Diversity:** Primary backup repository on a local storage server. A secondary copy that goes to the cloud hosted in a different region such as USA West. A tertiary immutable copy stored in a secure location.
* **Air Gap:** A weekly offline copy of backups that is completely detached from any network or power source. Such as a tape copy or offline object.
* **Regional risk management:** Off-site regions must be chosen to avoid natural disasters such as flooding or cyclones.
* **Encryption:** Backups must be encrypted, both in transit and at rest. Keys are to be stored in accordance with the password policy.

# Roles and Responsibilities

* **Principal:** Declares when a disaster has occurred, approves any necessary purchases and accepts any residual risks.
* **ICT Director:** Designs, runs and restores any backups. Maintains a recovery guide and leads any technical aspects of recovery.
* **Business Manager:** Staff and Parent communications, liaison with vendors, procurement for new hardware/personnel.
* **Privacy Officer:** Assesses breaches and determines if the OAIC must be informed of a breach.
* **Other Staff:** Report any incidents, comply with instructions.

# Recovery Priority Order

1. **Identity and access services** (Google accounts, SSO, access)
2. **Core networking** (firewall, routing, dhcp/dns, WiFi controllers)
3. **File share and Email** (Gmail, google drive, any network file transfers)
4. **Security tools and logs** (monitoring and logging)
5. **Printing services/IoT** (includes printers, scanners, cameras, sensors and other IoT devices)
6. **Low risk/Misc** (these are things which the school can still function normally without)

# Exemptions

Any exemption must be approved by the principal in writing, include a compensation for the exemption and also be time limited pending review.

# **Review**

This policy is to be reviewed annually and updated in order to match best practices. Furthermore, it may be reviewed in the event of any incidents or changes in technology or regulations.