MANA ACADEMY

CYBERSECURITY AND INFORMATION SECURITY POLICY

1. Purpose

Mana Academy recognizes its responsibility to protect student, employee, financial, operational, and other confidential information from unauthorized access, disclosure, alteration, destruction, or disruption.

The purpose of this policy is to establish a comprehensive cybersecurity program for Mana Academy that protects the confidentiality, integrity, and availability of school information systems and data and complies with applicable federal and Utah laws, administrative rules, and cybersecurity requirements applicable to local education agencies.

Mana Academy shall maintain cybersecurity practices based on a recognized cybersecurity framework and appropriate to the school's size, resources, technology infrastructure, and risk profile.

2. Authority and Legal References

This policy is adopted consistent with applicable law and regulation, including:

- Utah Code Title 53E, Chapter 9, Student Privacy and Data Protection;
- Utah Administrative Rule R277-487, Public School Data Confidentiality and Disclosure;
- Utah Government Data Privacy Act, as applicable;
- Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 C.F.R. Part 99;
- Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. § 1232h;
- applicable Utah cybersecurity and data breach requirements;
- requirements and guidance issued by the Utah State Board of Education (USBE); and
- other applicable state and federal cybersecurity, privacy, and records requirements.

Mana Academy shall update its cybersecurity practices as state requirements, administrative rules, or recognized cybersecurity standards are revised.

3. Scope

This policy applies to:

- all Mana Academy employees;
- administrators;
- Governing Board members when accessing school systems or information;
- contractors and consultants;
- volunteers with authorized access to school systems or confidential information;
- students using Mana Academy technology resources;
- third-party vendors with access to Mana Academy systems or data; and
- all school-owned or school-managed computers, mobile devices, networks, applications, cloud services, databases, accounts, and information systems.

This policy also applies to personally owned devices when those devices are authorized to access Mana Academy systems, accounts, or confidential information.

4. Cybersecurity Framework

Mana Academy shall implement and maintain a cybersecurity program based primarily on the Center for Internet Security Critical Security Controls (CIS Controls) or another comparable recognized cybersecurity framework approved by the Information Security Officer.

The cybersecurity program shall be implemented based on Mana Academy's size, available resources, infrastructure, operational needs, and risk profile.

At a minimum, the cybersecurity program shall address:

1. identity and access management;
2. hardware, software, system, and data asset management;
3. data protection;
4. security monitoring and logging;
5. vulnerability management and software patching;
6. incident response and recovery;
7. cybersecurity awareness and training;
8. third-party and vendor risk management;
9. network security;
10. backup and disaster recovery; and
11. cybersecurity governance and oversight.

5. Cybersecurity Governance and Responsibility

A. Governing Board

The Mana Academy Governing Board shall provide oversight of the school's cybersecurity program and shall:

- approve this policy and material revisions;
- receive periodic information regarding significant cybersecurity risks or incidents, as appropriate;
- support reasonable cybersecurity safeguards and resources; and
- ensure that school administration establishes procedures necessary to implement this policy.

The Governing Board is not responsible for day-to-day management of cybersecurity systems.

B. Executive Director or Designee

The Executive Director or designee shall ensure that Mana Academy implements this policy and assigns appropriate personnel to manage cybersecurity responsibilities.

C. Information Security Officer

Mana Academy shall designate an Information Security Officer (ISO) responsible for coordinating the school's information security program.

The Information Security Officer's responsibilities include:

- implementing and maintaining Mana Academy's cybersecurity framework;
- identifying and evaluating cybersecurity risks;
- coordinating security controls and safeguards;
- overseeing cybersecurity incident response;
- coordinating vulnerability assessments and remediation;
- maintaining or overseeing technology asset inventories;
- coordinating cybersecurity training;
- reviewing vendor cybersecurity risks;
- coordinating with Mana Academy's Data Manager;
- serving as a point of contact with USBE and other appropriate state cybersecurity resources; and
- maintaining cybersecurity documentation required by state law or rule.

The Information Security Officer may be an employee, contracted service provider, or other individual designated by Mana Academy.

D. Student Data Manager

Mana Academy shall designate a Student Data Manager as required by Utah law. The Data Manager and Information Security Officer shall coordinate concerning the collection, storage, use, disclosure, transmission, retention, destruction, and security of student information.

6. Asset Management

Mana Academy shall maintain a reasonable and current inventory of technology assets that access, process, transmit, or store school information.

The inventory should include, as appropriate:

- computers and laptops;
- servers;
- network equipment;
- mobile devices;
- school-issued student devices;
- software and applications;
- cloud-based services;
- databases;
- administrative information systems; and
- other technology capable of accessing school systems or confidential information.

Unauthorized hardware, applications, browser extensions, cloud services, or other technology may not be installed or connected to Mana Academy systems when doing so creates an unreasonable cybersecurity or data privacy risk.

Obsolete or unsupported systems shall be replaced, removed, isolated, or otherwise appropriately protected based on risk and available resources.

7. Identity and Access Management

Access to Mana Academy information systems shall be limited to individuals with a legitimate educational, operational, or business need.

Mana Academy shall:

- assign individual user accounts whenever practicable;
- prohibit employees from sharing passwords or account credentials;
- use role-based or least-privilege access principles;
- periodically review user access rights;
- promptly disable accounts when employment or authorized access ends;
- modify access when an employee's responsibilities change;
- require strong passwords or other secure authentication methods;
- implement multi-factor authentication for administrative, financial, email, cloud, and other sensitive systems where technically available and appropriate; and
- restrict privileged or administrator-level accounts to authorized personnel.

Employees, aides, and volunteers may not share or disclose passwords used to access student performance data or personally identifiable student information.

8. Student and Confidential Data Protection

Mana Academy shall protect personally identifiable student data and other confidential information throughout its lifecycle.

Student enrollment information, performance information, personally identifiable student information, and other protected data shall be collected, maintained, stored, accessed, transmitted, and destroyed securely and consistently with Mana Academy's adopted cybersecurity framework.

Reasonable safeguards shall include, where appropriate:

- encryption of sensitive information during transmission;
- encryption of sensitive stored information when reasonably available;
- access controls;
- secure file sharing;
- secure electronic communications;
- restrictions on removable storage;
- secure destruction of records and devices;
- appropriate physical safeguards; and
- limiting collection and retention of confidential information to information reasonably necessary for legitimate educational or operational purposes.

Employees shall not store confidential student or employee information in unauthorized personal email accounts, personal cloud storage accounts, unapproved applications, or other systems not authorized by Mana Academy.

9. Network Security

Mana Academy shall implement reasonable controls designed to protect its network and information systems from unauthorized access and malicious activity.

Controls may include:

- firewalls;
- web and content filtering;
- malware and endpoint protection;
- network segmentation;
- secure wireless configurations;
- restricted administrative access;
- intrusion detection or similar monitoring tools;
- secure remote access;
- disabling unnecessary services; and
- other technical safeguards appropriate to Mana Academy's infrastructure and resources.

Access to administrative systems from outside Mana Academy's network shall be secured using appropriate authentication and security controls.

10. Vulnerability Management and Security Updates

Mana Academy shall maintain procedures to identify and remediate security vulnerabilities.

School-managed devices and systems shall receive security updates and patches within a reasonable period based on:

- the severity of the vulnerability;
- the likelihood of exploitation;
- the sensitivity of affected information;
- operational considerations; and
- available resources.

Critical security vulnerabilities presenting an immediate or substantial risk shall receive priority.

Mana Academy may periodically conduct vulnerability scanning, cybersecurity assessments, penetration testing, configuration reviews, or other security evaluations internally or through qualified third parties.

11. Security Monitoring and Logging

To the extent appropriate and technically feasible, Mana Academy shall maintain security logging and monitoring for systems containing sensitive or critical information.

Security logs may be used to:

- identify unauthorized access;
- investigate suspicious activity;
- detect malware or compromised accounts;
- investigate cybersecurity incidents;
- identify attempted attacks; and
- support incident response and recovery.

Access to security logs shall be limited to authorized individuals.

12. Email, Phishing, and Social Engineering

Employees shall exercise reasonable care when using email and electronic communication systems.

Employees shall:

- avoid opening suspicious attachments or links;
- verify unusual requests involving money, passwords, employee information, student information, or account changes;
- report suspected phishing attempts;
- never provide passwords or multi-factor authentication codes in response to an unsolicited request; and
- independently verify unusual financial or account-change requests before acting on them.

Requests involving changes to payroll, direct deposit, banking information, vendor payment information, or other financial transactions shall be independently verified using a trusted method before the change is processed.

13. Cybersecurity Training

Employees and administrators shall receive cybersecurity and student data privacy training appropriate to their responsibilities. Training shall occur at hire or assignment and periodically thereafter.

Training should address, as applicable:

- password and authentication security;
- phishing and social engineering;
- email security;
- protection of student information;
- FERPA and Utah student privacy requirements;
- appropriate use of school technology;
- safe handling of confidential information;
- ransomware and malware;
- cybersecurity incident reporting; and
- emerging cybersecurity threats.

Employees authorized to access education records shall complete student privacy training and certifications required by Utah law.

Mana Academy may conduct periodic simulated phishing exercises or other cybersecurity awareness activities.

14. Third-Party Vendors and Service Providers

Mana Academy shall evaluate cybersecurity and privacy considerations before allowing a third-party vendor access to confidential information or school information systems.

Contracts involving protected student information shall comply with applicable Utah student data protection requirements.

When appropriate, Mana Academy shall consider whether a vendor:

- maintains reasonable cybersecurity controls;
- limits access to authorized personnel;
- encrypts sensitive information;
- maintains incident response procedures;
- promptly reports security incidents or breaches to Mana Academy;
- maintains appropriate data backup procedures;
- appropriately deletes or returns Mana Academy information at the conclusion of the contract; and
- complies with applicable student privacy and data protection laws.

A vendor or service provider shall notify Mana Academy promptly of an actual or suspected security incident involving Mana Academy information.

Mana Academy reserves the right to suspend or terminate system or data access when a vendor presents an unreasonable cybersecurity risk.

15. Backup and Disaster Recovery

Mana Academy shall maintain appropriate backups of critical information and systems necessary for school operations.

Backups shall be:

- performed at reasonable intervals;
- protected from unauthorized access;
- maintained separately from primary systems when reasonably practicable; and
- periodically tested or otherwise verified for recoverability.

Mana Academy shall identify critical systems and establish procedures for restoring operations following a cyberattack, equipment failure, natural disaster, or other significant disruption.

16. Cybersecurity Incident Reporting

All employees, contractors, and other authorized users shall promptly report suspected or confirmed cybersecurity incidents to the Information Security Officer, Executive Director, or designated technology administrator.

Reportable incidents include, but are not limited to:

- lost or stolen devices containing confidential information;
- unauthorized access to student or employee information;
- compromised passwords or accounts;
- phishing attacks resulting in account compromise;
- ransomware or malware;
- unauthorized disclosure of records;
- suspicious network activity;

- accidental transmission of confidential information to an unauthorized person;
- unauthorized system access;
- alteration or destruction of school information; and
- known or suspected vendor data breaches involving Mana Academy information.

Employees shall not attempt to independently investigate a serious cybersecurity incident unless authorized to do so.

17. Incident Response

Mana Academy shall maintain an incident response process appropriate to the nature and size of the school.

When a cybersecurity incident occurs, Mana Academy shall take reasonable steps to:

1. Identify the nature and scope of the incident.
2. Contain the threat and prevent additional unauthorized access or disclosure.
3. Preserve relevant records, logs, evidence, and documentation.
4. Eradicate malicious software, compromised credentials, vulnerabilities, or other causes of the incident.
5. Recover affected systems and restore normal operations.
6. Assess whether student, employee, financial, or other protected information was compromised.
7. Notify and report the incident to individuals and government entities when required by law.
8. Document actions taken in response to the incident.
9. Review the incident and implement appropriate corrective measures.

Mana Academy may obtain assistance from USBE, the Utah Cyber Center, the Utah Education and Telehealth Network, law enforcement, cybersecurity professionals, legal counsel, insurance carriers, or other appropriate resources.

18. Significant Student Data Breaches

A significant student data breach includes a breach in which:

- an intentional breach successfully compromises student records;
- a large number of student records are compromised;
- sensitive student records are compromised regardless of the number of affected records; or
- Mana Academy determines that the incident is significant based on the surrounding circumstances.

Mana Academy shall report a significant breach of student data involving Mana Academy or a third-party contractor to the Utah State Board of Education Superintendent within the timeframe required by Utah Administrative Rule.

Mana Academy shall provide required notice to an affected adult student or the parent or guardian of a minor student when required by Utah law.

The Information Security Officer and Data Manager shall coordinate required breach notifications and reporting, including reporting to the Utah Cyber Center or another governmental entity when required by applicable law, rule, or state directive.

19. Employee Responsibilities

All employees are responsible for helping protect Mana Academy information systems and data.

Employees shall:

- comply with this policy and related procedures;
- use school systems only for authorized purposes;
- protect passwords and authentication credentials;
- lock or secure devices when unattended;

- protect student and employee information from unauthorized disclosure;
- use only authorized systems for storing confidential information;
- promptly install required security updates on devices when directed;
- immediately report suspicious cybersecurity activity; and
- complete required cybersecurity and privacy training.

Failure to comply with cybersecurity requirements may result in limitation or removal of technology access and may result in disciplinary action consistent with Mana Academy policy and applicable law.

20. Personal and School-Issued Devices

School-issued devices shall be managed in accordance with Mana Academy security requirements.

Users may not intentionally disable or circumvent:

- endpoint protection;
- web filtering;
- device management;
- security software;
- access restrictions; or
- other cybersecurity controls.

Personally owned devices may only access Mana Academy information or systems when authorized and when reasonable security safeguards are maintained.

Mana Academy may restrict or prohibit personally owned devices from accessing sensitive systems.

21. Remote Access and Remote Work

Employees accessing Mana Academy systems remotely shall use approved methods and take reasonable precautions to protect school information.

Confidential information shall not be accessed through insecure public computers or stored on unauthorized devices.

Remote access to sensitive administrative systems may require multi-factor authentication or other additional security safeguards.

22. Artificial Intelligence and Emerging Technology

Employees may not enter personally identifiable student information, confidential employee information, financial information, passwords, protected records, or other restricted Mana Academy information into publicly available artificial intelligence systems or other unapproved technology platforms unless the service has been reviewed and approved for the intended use.

Artificial intelligence applications and emerging technologies that collect or process student information shall be reviewed under the same privacy, security, and vendor requirements applicable to other educational technology services.

23. Data Retention and Secure Destruction

Mana Academy shall retain records consistent with applicable state records retention requirements, education requirements, litigation holds, and Mana Academy's records policies.

When information is no longer required to be maintained, confidential records and data shall be securely destroyed or deleted in a manner intended to make the information irretrievable in the ordinary course of business.

Devices containing confidential information shall be securely erased or physically destroyed before disposal, sale, transfer, or reuse when appropriate.

24. Annual Cybersecurity Review

At least annually, the Information Security Officer or designee shall review Mana Academy's cybersecurity program.

The review should consider:

- significant cybersecurity incidents occurring during the prior year;
- changes in cybersecurity threats;
- security vulnerabilities;
- hardware and software inventory;
- administrative and privileged user access;
- staff cybersecurity training;
- backup and recovery capabilities;
- vendor cybersecurity risks;
- security improvements completed during the year;
- recommended improvements for the upcoming year; and
- changes in applicable federal or Utah cybersecurity requirements.

The Information Security Officer shall communicate significant cybersecurity risks or recommended improvements to the Executive Director and, when appropriate, the Governing Board.

25. Annual State Reporting and Compliance

Mana Academy shall provide USBE with required cybersecurity and privacy information by the deadline established by Utah Administrative Rule, including the name and contact information of Mana Academy's designated:

- Student Data Manager; and
- Information Security Officer.

Mana Academy shall maintain evidence demonstrating implementation of:

- applicable student privacy requirements;
- applicable data protection requirements; and
- an approved cybersecurity framework.

The Information Security Officer and Data Manager shall monitor guidance issued by USBE and modify Mana Academy's practices as necessary to remain compliant with current requirements.

26. Cybersecurity Implementation Plan

Because cybersecurity requirements and technology risks change over time, Mana Academy may implement cybersecurity controls in phases based upon:

- the school's size;
- risk level;
- available resources;
- existing infrastructure;
- technical feasibility; and
- the sensitivity of affected information.

High-risk systems and vulnerabilities shall receive priority.

A phased implementation approach does not relieve Mana Academy or its employees from complying with cybersecurity or privacy measures expressly required by applicable law or administrative rule.

27. Exceptions

Exceptions to this policy may be authorized by the Executive Director or Information Security Officer when:

- there is a legitimate educational or operational need;
- the exception does not violate applicable law;
- cybersecurity risks have been evaluated; and
- reasonable alternative safeguards are implemented when appropriate.

Significant exceptions should be documented.

28. Periodic Review and Policy Updates

This policy shall be reviewed at least annually and whenever significant changes occur in:

- applicable federal or state law;
- Utah Administrative Rules;
- USBE cybersecurity requirements;
- Mana Academy's technology environment; or
- recognized cybersecurity standards.

The Executive Director may approve administrative procedures and technical standards necessary to implement this policy without requiring Governing Board amendment of the policy, provided the procedures are consistent with this policy and applicable law.

Material changes to this policy shall be submitted to the Governing Board for approval.

POLICY ADMINISTRATION

Responsible Administrator	Executive Director
Information Security Officer	Assistant Director
Student Data Manager	Assistant Director
Technology/IT Provider	BoTecha
Approved by Mana Academy Governing Board on	