## Introduction

As an organization that seeks to aid in the improvement of educational outcomes for all children, NWEA is committed to maintaining the confidentiality, integrity, and availability of NWEA information assets and resources, including, but not limited to, the data of our partners. In doing so, NWEA information security controls are guided by the following principles:

- Protect the confidentiality, integrity, and availability of NWEA information assets and those of our partners.
- Comply with applicable privacy and data protection laws.
- Enable the business to make informed decisions through risk assessments.
- Grant access to sensitive, proprietary, or other confidential information only to those with a need to know.
- Provide security training opportunities and expert resources to help individuals understand and meet their information security obligations.
- Utilize the controls established by the National Institute of Standards and Technology (NIST) and applicable federal and state laws as guidance for our information security initiatives.

## Organizational security

### Employee background checks

NWEA utilizes a third party to conduct pre-employment background screening. As a condition of employment, all final candidates undergo national sex offender registry check, education verification, social security validation, and national criminal background checks.  Additional screening and checks are performed on individuals that access to sensitive areas.

### Security training for all employees

All NWEA employees undergo general information security awareness training as part of the onboarding process and receive ongoing security training throughout their NWEA careers. During the onboarding process, new employees agree to our employee guide which, among other things, highlights our commitment to keep student and confidential information safe and secure. NWEA recognizes that dedicated employee engagement is a key means of raising security and privacy awareness. Additionally, certain roles (for example, software developers and architects) undergo additional information security training.

### Dedicated security team

NWEA has a dedicated security team that employs security and privacy professionals.  This team is tasked with maintaining and/or advising on NWEA's defense systems, developing security review processes, advising on and building security infrastructure, and implementing NWEA's security policies. NWEA's dedicated security team actively scans for security threats using industry standard tools, penetration tests, and security reviews.

### Workstation security

All workstations issued to NWEA employees are configured by NWEA to comply with our standards for security. These standards require all workstations to be properly configured, kept updated, and tracked.

NWEA's default configuration sets up workstations to encrypt data, have strong passwords, anti-virus software, and lock when idle for a specified amount of time.

### Privacy

NWEA honors the privacy of student information and recognizes the importance of protecting such sensitive information. NWEA treats personally identifiable student data according to applicable local laws that regulate securing the access, maintenance, and transfer of such data. Additional information on NWEA's privacy policy for student information can be found at: https://legal.nwea.org/nwea-privacy-and-security-for-pii.html

### External audit and compliance

On an annual basis, NWEA engages with an independent third-party auditing firm that reviews MAP Growth's compliance with the criteria for the Service Organization Control (SOC) 2 Trust Principals for Security and Availability. A copy of NWEA's most recent SOC 2 audit is available upon request provided the requestor signs a non-disclosure agreement or has a current Master Subscription Agreement on file.

### Supply Chain Risk Management

NWEA's Legal Services examines and classifies third party access to NWEA systems, data, personnel, and physical locations. As part of this process, the Legal Services department reviews third party security controls, policies and procedures, contractual representations, and insurance to determine whether industry standard information security controls are in place based on the type of access and/or data they have access to. Thereafter, access is only granted to third-parties that are approved by the NWEA Legal Services.

### Physical Security

All visitors and vendors to NWEA's headquarters must be admitted at the front desk and sign in using NWEA's electronic sign-in system. Photo identification is required for anyone who enters sensitive areas of the building. All external doors and stairwell entrances are monitored by closed circuit security cameras and require badge access. Security personnel are onsite during the hours of 4 p.m.– to 8 a.m. M-F and 24 hours on weekends and holidays.

### Business Continuity

NWEA conducts business impact analysis and risk assessments as part of its business continuity plan (BCP). NWEA's BCP addresses all key functions of MAP Growth. Detailed testing plans have been developed to ensure continued operation of MAP Growth. NWEA reviews its BCP annually.

### Risk Assessments

NWEA conducts ongoing risk assessments to enable improved decision making, planning, and prioritization through a structured understanding of opportunities and threats to maximize the use of resources.

### General Data Protection Regulation (GDPR)

As a data processor, NWEA understands its obligations to comply with the GDPR. We thoroughly analyzed GDPR requirements and put in place a dedicated internal team to drive our organization to meet them. Our ongoing initiatives can be found here: https://legal.nwea.org/nwea-map-growth-gdpr-overview.html

## Operational Security

### Vulnerability Management

NWEA administrates a vulnerability management process that actively scans (internal, external, application) for security threats using industry best tools.  The vulnerability team tracks and follows up on vulnerability remediation.  Once a vulnerability requiring remediation is identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks issues and follows up frequently until they can verify the issues were mitigated or remediated.

### External Third-Party Penetration Testing

On an annual basis NWEA engages with an independent third-party organization to perform network and application level external penetration tests. The results of the penetration test are prioritized and corresponding remediation plans are enacted accordingly.

### Malware prevention

NWEA utilizes up-to-date antivirus on systems connected to the NWEA network.

### Logging & Monitoring

NWEA's security team maintains a security information and event management system to provide real-time analysis of certain log data and alerts.

### Incident management

NWEA maintains an incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team, privacy professional, or designated incident commander logs and prioritizes it according to its severity. The process specifics courses of action, procedures for notification, escalation, mitigation, and documentation. NWEA's security incident management program is structured around NIST SP 800-61 Rev 2, Computer Security Incident Handling.

### Network Security

Network access to NWEA's production environment from open, public networks is restricted. NWEA deploys mitigations against distributed denial of service (DDoS) attacks at its network perimeter. Changes to NWEA's production network configuration are restricted to authorized personnel. NWEA utilizes Intrusion Detection / Intrusion Prevention (IDS/IPS) services. NWEA also employs web filtering solutions that provide another layer of security protection against known compromised sites and malware.

### Media Sanitization

NWEA uses NIST SP 800-88, Guidelines for Media Sanitization, as guidance for asset sanitization and disposal decisions based on the security categorization of the associated system's confidentiality.

### Logical Access

NWEA has implemented information security guidelines that define how internal data, systems, and resources are secured and protected from unauthorized access, attempted intrusions, and service interruptions. These policies address topics that include, but are not limited to, access control, authentication, and remote access control.

### Encryption in Transit and at Rest

NWEA encrypts all traffic in transit over public networks using current industry standard encryption protocols and algorithms. Sensitive data in NWEA’s MAP Growth production systems and backups are encrypted at rest.

### Disaster Recovery

NWEA maintains a disaster recovery (DR) plan specific to MAP Growth to ensure the protection and restoration of systems, facilities, and capabilities and to reduce the consequences of any unexpected or undesirable event or disaster. This DR plan is intended to not only reduce the severity of the effects of a disaster, but to permit a planned, timely response and eventual effective recovery. The goal is to restore NWEA Product Engineering operations as quickly as possible. Disaster recovery on MAP Growth is exercised annually.

### Backup

NWEA automates full hourly backups of MAP Growth to the secondary colocation facility. Additionally, database replications are conducted hourly using native database capabilities.

Additional questions regarding NWEA’s MAP Growth Security Whitepaper can be sent to legalservices@nwea.org.

NWEA Legal Services & Enterprise Information Assurance Team

Document Last Modified: June 12, 2019