Illinois Mathematics and Science Academy®

INFORMATION TECHNOLOGY SYSTEM

USE AND ENFORCEMENT OF STRONG PASSWORDS

PURPOSE

The purpose of this Information Technology System document is to inform all users of IMSA technology resources of the requirements to use strong passwords to access protected systems in accordance with IT industry best practices and State of Illinois guidelines.

AUTHORIZATION

The authorization to administer, modify and enforce the provisions in this document is granted to the IMSA Chief Information Officer (CIO) by the IMSA Board of Trustees via policy **GBID Information System Technology Policy**. Therefore, this document may be changed as necessary to align with IT industry best practice without specific approval from the IMSA Board of Trustees. IMSA account holders will be notified as appropriate when changes are made.

SCOPE

This document applies to all IMSA staff, faculty and guest account holders, including but not limited to parents, alumni, board members, outside contractors and professional participants in external programs. As appropriate, it also applies to participants who remotely access virtual learning environments.

USE AND ENFORCEMENT OF STRONG PASSWORDS

Passwords are an important aspect of computer and network security. They are the front line of protection from network intrusion, protection of user accounts, and ultimately, protection of IMSA's data. A poorly chosen and maintained password can compromise the integrity of IMSA's entire system.

The password requirements below apply to all IMSA community members who have or are responsible for an account (or any form of access that supports or requires a password) on any system operated by IMSA ITS. These requirements also apply to any system that has access to the IMSA network, or stores any non-public IMSA information, regardless of its location.

- All IMSA accounts must use strong passwords in accordance with current IT best practices.
- All IMSA systems requiring login can only be accessed via encrypted connections in accordance with current IT best practices.
- Designated IMSA IT personnel reserve the right to test password strength using industry standard tools and methods.

- Accounts that do not meet the current strong password standards may be locked.
- All passwords must be changed on a regular basis in accordance with State of Illinois guidelines, IMSA ITS standards and IT industry best practices.

Password Requirements

- Passwords must be a minimum of eight (8) characters long.
- Passwords must be a mixture of upper and lower case letters, numbers and special characters (!@#$%^&*, etc.).
- Passwords may not be reused within a cycle of six changes.
- Passwords must not be a word that appears in any dictionary in any language, forwards or backwards, or any word of slang or jargon.
- Passwords must not be shared between users, at any time, in any circumstance.
- Passwords must never be communicated to anyone claiming to need them for purposes of verification of identity.
- Passwords must not be written down and stored in insecure locations.
- Passwords must not be communicated via email.

ENFORCEMENT

All rules and procedures in this document are enforced by the IMSA CIO. Any user of IMSA technology resources found to be in non-compliance with the provisions in this document is subject to disciplinary action under Board of Trustees policy GBDA. Such action can include one or more of the following, as appropriate: loss of the privilege of access (through suspension of system privileges or account termination), referral to law enforcement authorities, and/or disciplinary consequences, up to and including termination of employment.

EXCEPTIONS

Exceptions to this policy can be made only upon case-by-case review by the IMSA Chief Information Officer, the IMSA Director of Human Resources, or their designees.