Illinois Mathematics and Science Academy®

INFORMATION TECHNOLOGY SYSTEM

IMSA ACCOUNT RETENTION STANDARDS FOR NON-STUDENT USERS

PURPOSE

The purpose of this Information Technology System document is to inform all non-student and alumni users of IMSA technology resources of the rules concerning access to IMSA IT resources after leaving the Academy.

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, board members, outside contractors and professional participants in external programs. As appropriate, it also applies to participants who remotely access virtual learning environments.

ACCOUNT RETENTION

IMSA staff, faculty and external users are not allowed to retain their IMSA accounts after leaving IMSA (retirement, resignation, dismissal, sunset date, etc.). Unless otherwise authorized and approved by IMSA Human Resources, all non-student accounts are deactivated immediately or as soon as possible after the account holder separates from IMSA. The ownership of all data (email, documents, calendar data, etc.) left on the system by the account holder is transferred to the supervisor of record at the time of separation.

The accounts of employees who have been granted emeritus status are retained along with all appropriate privileges.

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.