Illinois Mathematics and Science Academy®

INFORMATION TECHNOLOGY SYSTEM

REMOTE ACCESS PROCEDURES

PURPOSE

The purpose of this Information Technology System document is to inform all users of IMSA technology resources of requirements and rules for accessing the IMSA network remotely via a Virtual Private Network (VPN) connection.

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 Polic**y. 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.

REMOTE ACCESS

Remote access to IMSA technology resources through Virtual Private Network (VPN) connections enables offsite users to operate as if they were connected to the network on-campus. Secure VPN connections are provided to those users with IMSA accounts, and those whose work requires or allows access from offsite.

Remote access has been instituted to advance the work of the Academy. It is an enhancement to the network services, offering an alternative method of entry for those who must perform all or some of their work from off campus

To enable this access, IMSA ITS will install approved VPN software on Academy-owned equipment. VPN access by non-Academy owned equipment is not allowed.

It is the responsibility of IMSA employees, contractors, vendors and agents with remote access privileges to the IMSA network to ensure that their remote access connection is operated in accordance with all other IMSA policies.

The remote user bears responsibility for the consequences if the access is misused.

While connected to the IMSA network via VPN, the remote computer will be unable to access the public Internet (no “split-horizon”).

Remote access is available to:

- All current employees and Board members of the Academy
- All current contractors of the Academy, if such access is contractually required
- All other valid account holders, including students, may be granted remote access on a case-by-case basis

Access will only be granted to those who have specific IMSA responsibilities which advance the mission and work of the Academy and for which other access means are not available or practical

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.