Illinois Mathematics and Science Academy®

INFORMATION TECHNOLOGY SYSTEM

SECURITY AWARENESS

PURPOSE

The purpose of this Information Technology System document is to inform all users of IMSA technology resources of the common methods used in attacks against computers and networks. Increasing awareness of potential threats can greatly reduce the number of security related incidents.

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.

SECURITY AWARNESS FOR IMSA IT

Research has shown** that increasing awareness of threats can greatly increase the overall effectiveness of IT system security. In keeping with best practice in this area, IMSA has developed presentations designed to illustrate the most common forms of exploits that target the human elements of computing systems. These materials are available on the IMSA web site at https://www.imsa.edu/discover-imsa/operations-and-support-services/its/ and can be reviewed by all IMSA account holders at any time.

All IMSA employees are required to attend a presentation covering security awareness, as it relates to the use of IT resources, before they receive access to their assigned account. This is part of the employee on-boarding process. In addition, all employees may be required to take periodic refresher training.

IMSA IT may randomly send messages to IMSA staff and students designed to test the effectiveness of our training materials. The test results will also help us keep the training materials up to date. At no time will the test results be made public. Based on the results, we may contact IMSA staff and students for further training.

** http://csrc.nist.gov/organizations/fissea/2012-conference/presentations/fissea-conference-2012_quagliata.pdf

http://www.tandfonline.com/doi/full/10.1080/19393555.2012.747234

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.