

## Walsh College Information Technology Security Policy

### 1. Overview

Walsh College relies heavily on Information Technology to meet its educational, financial, and operational objectives. It is therefore imperative that data, hardware, networks and software be sufficiently protected against modification, damage, theft or unauthorized access.

### 2. Purpose

The purpose of this policy is to establish and communicate mandatory Information Technology requirements to safeguard Walsh College's Information Technology and electronic information.

### 3. Policy

Walsh College will protect its Information Technology assets, including its networks and data, by controlling authorized access, creating logical and physical barriers to unauthorized access, configuring its hardware and software to protect its networks and applications, and by monitoring network activity. These measures will apply to employees, students, contractors, business partners or other third parties who connect to the Walsh network or other information technology system. This includes remote access connections to the Walsh network.

Only authorized individuals may access a Walsh College information technology asset. Access will be granted according to business or academic need after proper system approval by the appropriate college office that is responsible for the data or system to which access is requested. Confidential or sensitive data may only be stored on information technology assets owned by Walsh College. Guests may obtain temporary system credentials to access public resources through the Walsh College kiosks located throughout the campuses.

### 4. System and Data Security

Walsh College will design its network architecture and applications to limit user access to only those systems or data required to meet an academic or business need. Walsh College will secure data centers, switch rooms and other sensitive sites against unauthorized physical entry, and will construct perimeter networks or other hardware configurations to control access, including remote network access, to applications or other information technology systems.

Walsh College will configure its hardware and software to eliminate known security vulnerabilities and will apply vendor certified software patches promptly. It will filter and scan incoming email messages and files for viruses, worms and other malicious programs.

Walsh College will use change management tools to monitor, evaluate and record alterations to an existing production environment, e.g., a change to program code or a configuration change to software or hardware. The degree of review the change receives will be determined by its impact on other Walsh College information systems or users.

Walsh College will further protect its data and networks by backing up data according to industry-accepted standards. As required, Walsh College will create and maintain redundant systems, and plan appropriate measures to recover its information technology assets from disaster or other significant interruption of service.

Walsh College will use intrusion detection technology, engage outside consultants to perform security reviews and identify and assist application data owners with their review of access to financially or otherwise significant college systems. Walsh College will investigate identified exceptions to this policy and report such exceptions to appropriate offices as required.

Walsh College will follow industry-accepted standards for cybersecurity preparedness and response planning, such as those outlined in the Framework for Improving Critical Infrastructure

Cybersecurity published by the National Institute of Standards and Technology. Walsh College will perform regular audits of its cybersecurity preparedness.

**5. Privacy**

Walsh College will comply with its written privacy policies and with the requirements of the Federal Educational Rights and Privacy Act.

**6. Education and Awareness**

Walsh College will provide mandatory information technology and awareness training for its employees, students, contractors, business partners or other third parties who connect to the Walsh network or other information technology system.

Walsh College will provide a manual to its students to educate them on best practices relating to information technology and security.

Walsh College will promote information technology security by posting policy reminders and banners on computers and around campus where appropriate.

Walsh College will provide a help desk or online resources to assist students and the user community with information technology and security-related issues.

**7. Information Technology Department**

Walsh College will have in place one or more persons to assist with information security at the college. Walsh College will provide contact information and availability of the Information Technology Department team to the Walsh College user community.

At present, the following individuals are responsible for information security:

Helen Kieba-Tolksdorf - [Vice President, Chief Financial Officer and Treasurer](#)

Jacob Klein – Executive Director of Information Technology