Saint Michael's College

Information Security Policy:
Personnel Security Guidelines

1. Purpose

To ensure access is deleted in a timely manner for terminated employees, and modified appropriately for transferred or promoted employees. This guideline is intended to provide a framework by which a Saint Michael's College (SMC) department can ensure security controls are implemented to protect the privacy, security and integrity of SMC information technology resources against unauthorized or improper use, and to prevent and detect attempts to compromise information technology resources for any terminated, transferred, or promoted employees.

2. Scope

All SMC departments must establish and document the process which directs the steps and the timing required to grant and withdraw physical and system access privileges to personnel for the following events: new hire, employee transfer to another SMC department, employee termination, employee resignation, employee change of job duties within a Saint Michael's College department, and perceived disgruntled employee behavior. The following guideline provides the standard framework for creating this process.

Guidelines:

Personnel security begins during the staffing process. Once personnel have been staffed, personnel security safeguards are administered according to SMC security policy and acceptable use agreements via a college defined User account management procedure. User account management involves 1) establishing the procedures for requesting, issuing, and closing user accounts over the life cycle events of personnel (e.g., initial hire, transfers, position promotion, retirement, resignation, etc.); 2) tracking users and their respective access authorizations; and 3) managing these functions on an on-going basis.

The following are the minimum steps recommended to be included in the procedure for administering personnel security access:

New Hires: (Teaching Faculty, Administrators, Adjuncts, Part-time and Student Employees)

a. The Human Resources Office and the immediate supervisor are responsible for notifying the Information Technology Department (IT) of any new hires that require access to Mikenet. This information should be formally communicated prior to employee's assigned start date.
b. All employees must sign SMC Mikenet Account Agreement immediately upon employment with the college.
c. The immediate supervisor should determine the type of computer access that is needed for each employee and the sensitivity/confidentiality of the information/data required for that position. Access granted to personnel must be based on least privilege (i.e., only up to the level needed to perform one's duties).
d. Employees must attend security awareness training programs offered by the college.
e. IT is responsible for granting the access as authorized by the employee's immediate supervisor. They are expected to maintain formal records for any approved action and

provide the immediate supervisor access to those records as required. This step should be automated where feasible.

Employee Transfer:

a. The responsible supervisor must determine the type of computer access that is needed for each employee and the sensitivity of the information/data required for that position.
b. IT should work with both the present and former supervisors to modify the employee's logical and physical access to meet the needs of the new position.
c. IT is responsible for granting the access as authorized by the employee's immediate supervisor. They are expected to maintain formal records for any approved action and provide the immediate supervisor access to those records as required. This step should be automated where feasible.

Employee Promotion:

a. The immediate supervisor must review current access and determine the type of computer access that is needed for the employee and the sensitivity of the information/data required for that position.
b. IT will work with the supervisor to modify the employee's logical and physical access to meet the needs of the new position.
c. IT is responsible for granting the access as authorized by the employee's immediate supervisor. They are expected to maintain formal records for any approved action and provide the immediate supervisor access to those records as required. This step should be automated where feasible.

Employee Separation:

a. The immediate supervisor and the Human Resource Office must formally notify IT when employees are separated from service or end their employment. In cases of abnormal terminations (firing, death, etc.) the notification should be handled with urgency.
b. The department must also address and make considerations for employees who are not officially separated but may not be active for a specified period of time such as adjunct faculty.
c. IT is responsible for granting the access as authorized by the employee's immediate supervisor. They are expected to maintain formal records for any approved action and provide the immediate supervisor access to those records as required. This step should be automated where feasible.

Review and Certification of Access:

Each department should consider the following steps in creating the internal procedure for reviewing and certifying the employee's continuing need for access to SMC information technology resources:

a. All supervisors are solely responsible for auditing/recertifying, where applicable, the access of all of their direct reports including Faculty, Administrators, Student Employees, Adjuncts, and consultants during the college-wide Information Security Plan review each July. Failure to provide notification could result in the individual's access being automatically being suspended or in some cases revoked.
b. IT will formally notify departments of any security changes impacting enterprise applications/services.

3. Definitions

Personnel Security refers to those practices, technologies and/or services used to ensure that personnel security safeguards are applied. Personnel security safeguards take into account 1) granting or withdrawing physical and system access privileges upon: hiring an employee, transferring an employee to another SMC department, terminating an employee, or when an employee resigns or changes job duties within a SMC department; 2) system access will be granted, modified and revoked via a formal and auditable process, 3) Background checks of personnel may be required consistent with SMC Human Resources policy and depending on the sensitivity of information accessible to that position.

Auditable Process refers to specific documentation which can be a manual or an automated process that provides sufficient evidence that will allow one to trace the events of an action that has taken place.

Sensitive Data/Information refers to critical information for which the unauthorized access, loss, misuse, modification, or improper disclosure could negatively impact the ability of SMC to provide services and benefits to its students.

Confidential Data/Information refers to information that involves the privacy to which individuals are entitled by law. This information may only be disclosed to those individuals that are authorized and have a need to review the data or information.