ST MARY'S
COLLEGE of MARYLAND
The Public Honors College

OFFICE OF INFORMATION TECHNOLOGY
47645 College Drive
St. Mary's City, MD 20686

www.smcm.edu
TEL: 240-895-4357

SMCM Computer Administrative Rights Policy

Purpose

This document defines the policy regarding local administrative rights for faculty and staff on St. Mary's College of Maryland PC/Mac computers.

Introduction

By default, all Faculty and Staff are provided standard user rights on their college assigned PC/Mac computer, and rely on the IT Support Center for software installations and/or system modifications. This is a security best practice consistent with the "USM Guidelines in Response to the State IT Security Policy". Restricting user level administrative rights can dramatically reduce the risk of malware infections. Malware on an infected machine will typically gain the same access rights as the logged in user account, and if that account has administrative rights, then the malware has the potential to do much more damage.

Applying for an Administrative Account

Administrative rights are typically restricted to system and network administrators within the Office of Information Technology. However, faculty and staff can request and receive administrative rights in a temporary or ongoing basis when the elevated rights are routinely required for the individual's role or job responsibilities.

For audit purposes, SMCM must maintain documentation showing that a request for a local administrative account has been formally approved.

To apply for a local administrative account, please complete and sign the Administrative Rights Request Form.

Requests are approved by the Assistant Vice President of Information Technology. The user will be notified of the decision within ten days of submitting the request.

Administrative Rights Responsibilities

Faculty and staff who request administrative rights understand the responsibility of maintaining appropriate security measures to protect SMCM computing resources and data.

If administrative rights are approved, you will be provided a local user account with the elevated privilege. Your network account will maintain standard user level privileges and you must continue to log into your computer using this network account. When performing a task that requires elevated privilege, you will be prompted to provide your local account credentials. It is very important that you stay logged into your computer with your network account. System and network administrators within the Office of Information Technology also follow this security best practice.

Users will be required to change the password of their local administrative and network accounts every 90 days.

Users must NOT

- download and install software that is malicious to the SMCM network;
- download and install illegal or unlicensed software;
- download and install software not related to SMCM business;
- create additional user accounts;
- circumvent user access controls or any other security control instituted by the Office of Information Technology.

Users who do not adhere to the administrative rights responsibilities will have their local administrative account privileges revoked.

Standard Operating Procedures

If the Office of Information Technology is required to restore your computer, it will be restored to the standard configuration.

Your local administrator account will not transfer when you receive a new computer. If you continue to require a local administrator account, you will need to re-apply via the Administrative Rights Request Form.

Revision History

Version	Published	Author	Description
1.0	9/7/2016	Chris Burch	Original Publication