

Miami University
Guidelines for Obtaining Security Office Services

Index: SOPR-200501

For The Security Office
William L Custer
Version 1.1 – May 9, 2006

Guidelines for Obtaining Security Office Services

Introduction

Since security is everyone's responsibility it is sometimes difficult to know who is directly responsible for ensuring that particular Jobs are adequately secured. Security policies and standards exist across all departments of IT Services as well as across other departments of the University. Likewise, the Security Office has organization-wide responsibilities to ensure that secure practices are employed as well as to assist in their implementation.

To accomplish this, responsibility for securing university resources is also distributed across many layers of the University's reporting structure. Staff both inside and outside of IT Services are responsible to secure various servers, applications that run on them and the portions of the network that they touch.

Project Management methodology as practiced in IT Services adds an additional layer of complexity to the question of who is responsible for a particular security Job, since projects can also range across departments in IT Services as well as across other university departments.

Decisions impacting security can have far ranging implications. Trade-offs made for the needs of one system may adversely impact the security of others, so each project must recognize its needs with respect to the broader organizational security environment.

This document is intended to clarify selected security responsibilities in new projects, in Jobs that implement new services, and in daily operational Jobs.

Case One: Projects.

Project Management methodology places all aspects of the project under the leadership of the Project Manager until the project is closed. The Project Manger is responsible to deliver a service that not only works but also meets organizational requirements, among which is security.

All new services must meet a minimum set of security requirements, as stated in the document entitled "University Information Security Requirements" available in the Project Office. There may also be other security requirements placed on a service or a system by the Security Office. A security review may be recommended in some cases.

A Project Manager is not likely to be a security expert, therefore to meet these minimums and other security requirements, the Project Manager will need to lead his/her project team to do so. Since the Project Team will generally include a Technical sub-group of Subject Matter Experts who are familiar with technical details including general security requirements, it is assumed that there is available expertise. On some projects, however, a representative from the Security Office may be included as part of the project team to assist with security requirements.

Project security requirements could come from a number of sources including: the UISR document, Business Units, Federal or State Law, University Policy, or the Security Office itself. The project's subject matter experts will need to assist the Project Manager in applying security requirements to design "secure systems within secure environments using secure technical architectures".

Each project need not invent security solutions from the ground up, since prior projects may have useful solutions that can be reused. Other project managers, technical staff, and the Security Office can assist in finding existing security solutions that can be adapted to new services.

Project Managers and their projects are responsible to make provisions for the ongoing operational security needs of their service once it is placed into production and the Project Team is dissolved. At that time, security issues related to the service are handled as spelled out below under Case Three: Daily Operational Jobs.

Case Two: Jobs That Implement New Services

Many new services are delivered by IT Services or by other departments in the University without a project being formed. These are informally called 'Jobs'. In these cases the Job manager must assume responsibility to deliver a secure service based on the same guidelines that are given to Project Managers of formally declared projects.

Since no formal Job management methodology exists in either IT Services or the University, no Job manager is formally named by management. In Jobs that cross departments, several departments can assume Job leadership and appoint Job managers; the result of multiple Job managers can be that responsibility for big picture questions like security are forgotten.

Since the Security Office may not be aware that a Job is under way, the manager who commissioned the Job also has a responsibility to see that security requirements are met.

Case Three: Daily Operational Jobs

Daily operational Jobs are distinct from other Jobs in that they deliver no new service and are not part of some other larger project or Job where security implications will have been examined. Many operational Jobs like data backups are repeated, well-understood, and have a body of procedures to govern them; others may be one-time, poorly understood, or have no procedures at all! In either case, operational Jobs may have significant impact on organizational security and therefore should be carefully managed.

Daily operational Jobs are managed by the operational implementer (or by the manager who requested the work). The operational implementer is responsible to examine all security implications of the Job.

Some operational Jobs will be under change control and the change control board approval process may examine security implications. If the Job is not governed by change control, the operational implementer must take careful consideration to see that no security requirements are violated by the Job.

All Cases: One, Two, Three

Whether a service is implemented as a Project, a Job, or a Daily Operation, security requirement must be met. Security requirements could come from a number of sources including:

- University Information Security Requirements (UISR) – Available from the Project Office or Security Office Consultation
- Law
- University and Departmental Policy
- Business Units,
- Security Office.

Exceptions

Project managers, Job managers, and operational implementers may find that their proposed action may conflict with the requirements stated above. In this case, they can apply in writing to the Security Office for a temporary exception or exemption.

Written applications should be addressed to the CSO and include the reasons for the exception as well as a statement of risk that occurs from the exception. Examples of an application for exception and the statement of risk can be obtained from the Security Office and the Security Office web page. Higher levels of risk may need to be escalated to IT Services upper management (CIO, Leadership Team) to be fully resolved. This is usually accomplished in consultation with the security office.

Note: On September 29, 2005 this document was presented to IT Services staff in an open meeting. At that time Reid Christenberry endorsed the this document.