GENERAL			
Description	This is the policy that governs the Anti-virus Notice Policy and Procedures process under Computing Sector management.		
Purpose	This policy ensures a consistent, repeatable process that enables the Computing Sector to offer a high quality service to the Division Heads', Researchers, Experiment Leaders, and to our end-users.		
Applicable to	This document applies equally to all Fermilab Computing Sector personnel		
Supersedes	No previous version		
Document Owner	Computing Sector Head	**Owner Org**	Computing Sector
Effective Dates	12-10-2009 – xx-xx-xxxx	**Revision Date**	xx-xx-xxxx

VERSION HISTORY			
Version	**Date**	**Author(s)**	**Change Summary**
Draft 1.0	12-10-09	Greg Cisko	Initial draft
Draft 1.1	11-11-11	Jason Ormes	Password Reset Update

TABLE OF CONTENTS

1.0 GOAL AND OBJECTIVES

Provide a centrally managed and controlled anti-virus response with the goal of providing consistant and measurable service to the lab.
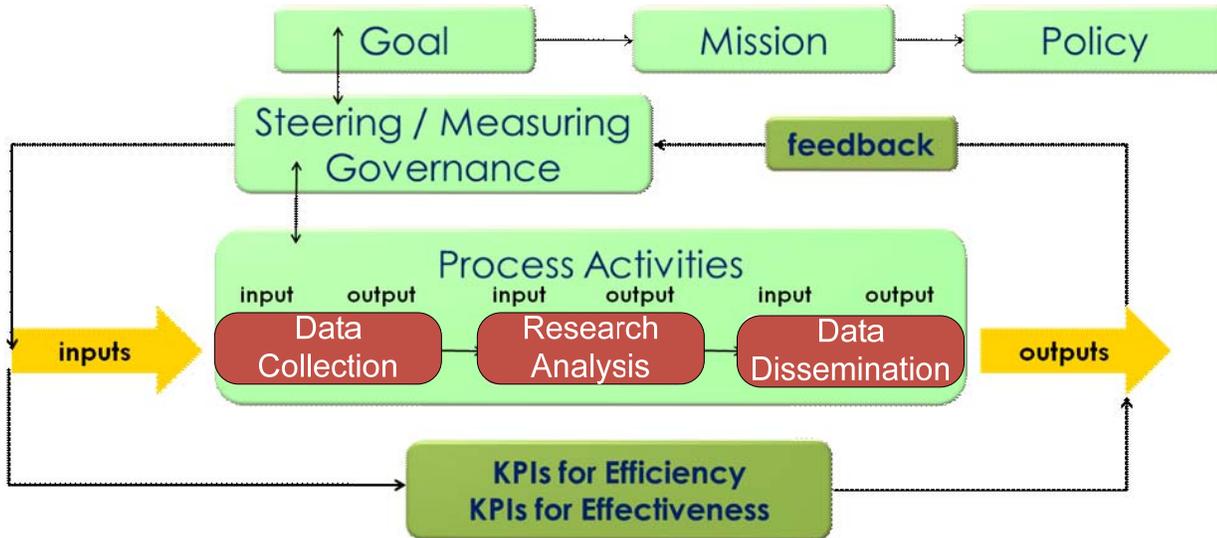
2.0 ANTI VIRUS NOTICE POLICY AND PROCEDURE OBJECTIVE

AV notices will be to either BLOCK a machine or simply NOTIFY.

- If the notice is NOTIFY, we ignore the machine and there is no further follow up.
- If the notice is BLOCK we will respond in 1 of 3 ways
  - If the virus location is in the System Restore area, we will attempt a fix by disabling System Restore and re-enabling it. This will remove all previous restore points on the machine, but is less invasive than wiping and reinstalling.
  - If the Virus location is in a system area other than System Restore we will wipe and reinstall as per our procedure.
  - If the Virus is of a critical type (e.g. Hacktool or info stealer), but is not in a system area, and looks like it was not executed or simply found in the zip file, we will do an offline scan.
    - If the scan finds nothing else, we will remediate the block and release the machine to the user.
    - If the scan shows additional virus infections, we will wipe and reinstall as per our procedure.
- When a wipe and re-install is determined necessary, we will expire the users SERVICES and FERMI passwords. The user can then reset the passwords at the servicedesk or desktop support area. (Note: these procedures are only invoked for systems on site and available to the desktop support team.)

Any notices that do not apply to the above procedure will cause an immediate review of the procedure to determine the best solution.

3.0 ENFORCEMENT

Individuals who violate this policy will be denied access to laboratory computing and network facilities and may be subject to further disciplinary action depending on the severity of the offense.

4.0 RELATIONSHIP TO OTHER DOCUMENTS	
Document Name	**Relationship**
ITIL Related process documents	Terms and Definitions
AV Tissue Detector	Procedure
Malware removal procedure	Processes
ITIL related policy documents (i.e. Service Catalog policy, Change Policy, etc.)	Policies
Miscellaneous related documents that are aligned or assist in the Incident Management process	Other
ITIL Glossary	Terms and definitions