PROJECT DOCUMENTATION

PROJECT PRE-INITIATION DOCUMENT

RHUL Desktop Antivirus Solution

Release: **Version 1.1**

Date: 9th[th] March 2007

Author: Huw Michael

Project Pre-Initiation Document History

Document Location

This document is only valid on the day it was printed

The source of the document will be found on the in the formal projects folder at:
\\pfs4\ccroot$\Project\Current\Desktop-Antivirus

Revision History

Date of this revision: 09/03/07
Date of Next revision: n/a

Revision date	Previous revision date	Summary of Changes
4/12/06	n/a	Draft
15/01/07	4/12/06	Amended selection method and order of phases
08/03/06	15/01/07	Change of title, restructure content, add outline delivery dates

Distribution

This document has been distributed to

Name	Title	Date of Issue	Version
Laura Gibbs	IT Director	4/12/06	Draft
Laura Gibbs	IT Director	15/01/06	1.0
John Kalogeras	Infrastructure Manager	09/03/06	1.1
IT Infrastructure Team		09/03/06	1.1
Judith Crocker	Head of User Support	09/03/06	1.1
John Gregory	User Support Officer	09/03/06	1.1

Project Initiation Document

Purpose of Document

The purpose of this document is to define the project, to form the basis for its management and the assessment of overall success.

Background

RHUL currently have an inadequate and unmanageable desktop antivirus solution which has a poor detection rate and is causing unnecessary work for IT staff in repairing mis-configurations and faulty update mechanisms. RHUL currently have no central reporting / management interface and therefore have no immediate view of client status in regard to the dates of viral definition files or the detection of known viruses.

RHUL have recently procured a reputable file based scanning solution for the server side and a separate mail scanning solution for the new Exchange 2003 servers. The SMTP mail gateways on the UNIX platform also employ a reputable open source scanner.

The RHUL systems team have elected to pursue a tiered solution for virus and malware protection whereby different solutions are implemented on the client and server side. This is considered good practice in industry.

This document recommends the procurement of a client side antivirus solution which can scale to provide generic Anti-X capability (anti-spyware, anti-phishing, potentially unwanted program detection). It will be installed widely across the campus infrastructure as a recommended IT services solution and must provide centralised management and reporting features.

Project Definition

Project Objectives

- To review the current desktop antivirus provision within Royal Holloway University of London
- To bring forward recommendations to procure, implement, and deploy a new solution
- To implement and deploy an agreed solution, to remove the old solution, to arrange a training programme for IT staff, to communicate the availability of a new solution to all relevant customers

Project Scope

- The provision of a desktop antivirus solution for all campus clients
- Investigation into the scalability of such a solution to incorporate Anti-X / Network Access Protection / Personal Firewall functionality
- Platforms – PC; investigate provision for Apple Macintosh, UNIX, Linux and others
- Consideration of provision and licensing for staff home use
- Consideration of provision and licensing for students home use

Method of Approach

- Consultation within the Computer Services department and with technical contacts
- Consultation and information gathering from other Universities
- Information gathering from suppliers, supplier presentations
- Formulate requirements specification for RHUL
- Issue “request for pricing” and requirements specification to vendors
- Evaluate and compare responses
- Select 1 solution for pilot / testing
- Implement across a range of desktops & users
- Evaluate fitness for purpose & collate feedback
- Select solution or test / pilot an alternative solution
- Procure & implement solution
- Communicate, train, roll out solution across campus

Project Deliverables and/or Desired Outcomes

Phase 1 – Consultation

Start Date – 12/03/07

- Report on outcome of consultations with IT Staff
- Report on outcome of consultations with departments and individuals
- Report on outcome of information gathering from other universities and vendor reference sites
- Report on outcome of information gathering from vendors
- Document requirements specification

End Date – 23/03/07

Phase 2 – Request for Pricing

Start Date – 26/03/07

- Issue request for pricing and requirements specification
- Produce matrix for evaluation of responses
- Collate responses and evaluate against matrix
- Rank solutions in order of preference / suitability
- Agree trial period and support with preferred vendor

End Date – 09/04/07

Phase 3 – Pilot Implementation and Testing

Start Date – 09/04/07

- Pilot system set up on test server, document installation and configuration
- Plan and document test strategy including installation scenarios
- Install client on selected RHUL desktops: Academic, ADMIN, PC Lab build etc
- Install client on example student desktop
- Install client on example staff home desktop
- Investigate removal mechanism for existing solution. Document procedure
- Test and evaluate deployment: Active Directory, foreign domains, workgroups etc
- Test and evaluate management console and delegation of administration / monitoring
- Evaluate and document hardware requirements for server provision

End Date – 30/04/07

Phase 4 – Procurement & Planning

Start Date – 30/04/07

- Agree on final solution and scope / licensing requirements
- Procure Antivirus solution and agree support terms / assisted installation
- Procure server hardware
- Plan implementation and rollout

End Date – 07/05/07

Phase 5 – Deployment, Documentation and Training

Start Date 07/05/07

- Implement server side of Antivirus solution and confirm documentation
- Plan phased rollout of solution across campus clients (including removal of old solution)
- Evaluate requirements for user training and IT staff training
- Produce systems and training documentation
- Plan communications and support mechanism for initial change
- Plan support mechanism for student use
- Deliver training to IT and technical staff
- Implement phased desktop rollout internally
- Deliver user training as required
- Communicate and distribute solution for home use
- Communicate licensing implications for home users of existing system

End Date – 4/06/07

Exclusions

This project aims to provide a means by which the University can implement a security policy and in future a network access protection policy, insisting on up to date antivirus provision as a condition of connectivity and support, but not to enforce exclusive use of this solution for student and staff home use.

Constraints

Limited staff resources, short time-scale from consultation to implementation

Assumptions

Available resources are adequate
Co-operation between teams within I.T. Services and between University departments and I.T. Services

Costs

Yet to be determined but will appear in the form of software licensing and server hardware.

Timetable

As outlined in the Project deliverables.
This equates to 2 months for selection and procurement, 1 month for implementation.

Communications Plan

Communications will be a major requirement for the consultation process and will be conducted by email and formal project documents.

Information about the project will be provided by email and by the project's formal documents, available via shared file space.

Stakeholders

Users (University Staff and Students)
IT Staff (Computer Centre staff and departmental technical staff)
Project Team
Suppliers

Information required

Technical & User requirements – will be obtained through consultation
Solutions available – will be obtained through a Request For Pricing (RFP)
Solution to be implemented – will be chosed further to evaluation of RFP and pilot.

Method of communication

Questionnaires
Consultation meetings
E-mail
Published documentation
Meetings

Change and Configuration Management

Change Management Procedures

Request for Change Form will be completed and submitted as appropriate

Configuration Management Plan

Hardware and software installation will be documented by staff who execute the procedures
Documents will be updated with subsequent changes to configuration
It would be desirable to produce a template for installation documentation to ensure uniformity and ease of use of this documentation
Documents will be stored centrally

Project Controls

Initial Risk Log

Limited cover if suffer loss of key staff (e.g. other employment, illness)
Objection to central antivirus provision from independently maintained departments
Compatibility of Antivirus solution with future operating systems e.g. 64-bit Vista
Training resources are available, and adequate
Delivery of hardware

Contingency Plans

Contractors can be hired to address staffing problems
Liaise closely with independent departments
Monitor market closely, discuss with vendors
Regular and close contact with training team to foresee any possible shortcomings
Training could be outsourced

Project Filing Structure

Documents located at:

\\pfs4\ccroot$\Project\Current\Desktop-Antivirus